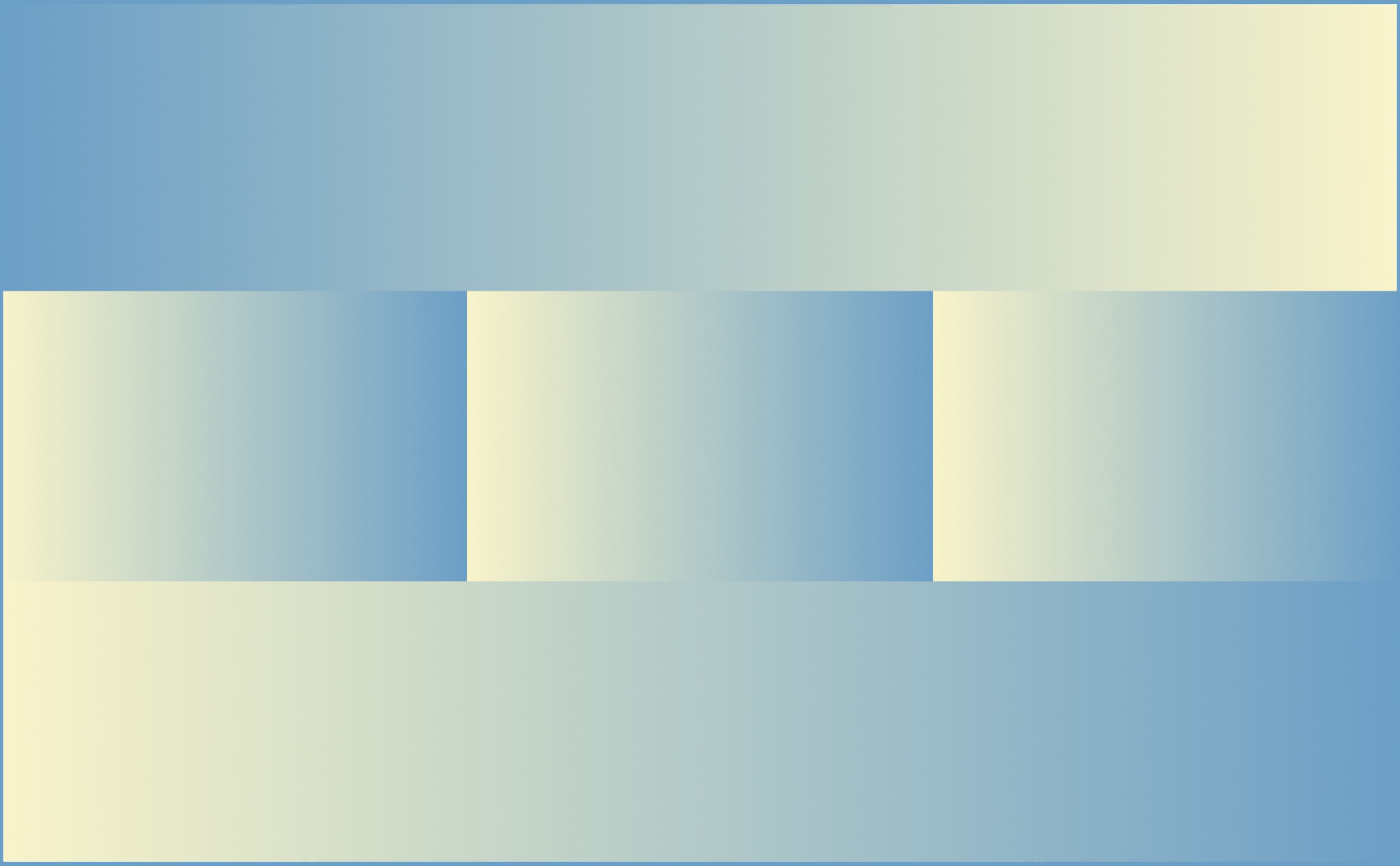

STUDY

The State of Cyber Confidence-Building Measures

How Governments Implement Multilateral Measures to Create Trust in the Cyber Domain

Helene Pleil

Dec 16th, 2025

Tech analysis and policy ideas for Europe

interface

Table of Contents

1. Executive Summary

Confidence-Building Measures in the Cyber Domain

In any political domain, building trust in international relations is essential, but in the cyber domain this is particularly true. Cyber interactions carry high risks of misunderstanding and escalation, as the environment is marked by uncertainty, ambiguity, and anonymity. Factors such as the difficulty of attributing incidents, the potential for false-flag operations, and rapid technological change further increase these risks.

These dynamics are intensified by today's geopolitical climate of rising tensions, strategic competition, and weakening alliances. In such a context, unintended cyber escalation can occur easily, making mechanisms that reduce uncertainty and foster trust all the more important.

Confidence-Building Measures (CBMs) serve this purpose by enhancing transparency, predictability, and dialogue through practical steps such as information-sharing, notification, and cooperation. They are not an end in themselves but a diplomatic tool to prevent escalation and sustain communication, especially in times of mistrust.

Cyber CBMs in Multilateral Organisations

This poses the question: how can confidence be built in a domain defined by ambiguity? Over the past decade, states have sought to answer this question through the negotiation and implementation of cyber CBMs in unilateral, bilateral, and multilateral settings. Among these, CBMs within multilateral organisations have proven especially effective and durable.

Regional organisations are well positioned to advance cyber CBMs as they account for differing levels of cyber maturity, political priorities, and cultural contexts. Compared to global forums, regional initiatives can offer more targeted solutions among states with shared threat perceptions. Their proximity to national authorities enhances understanding of national perspectives, while their membership – often including both like-minded partners and neighbours with strained relations – provides valuable platforms for dialogue. Building on established regional processes further strengthens their effectiveness. Examples of such regional cyber CBMs include establishing directories of national Points of Contact (PoCs), sharing cybersecurity strategies, exchanging national views on threats or on the application of international law in cyberspace, conducting joint workshops – often with the private sector, which owns and operates much of the ICT infrastructure – building national capacities, or setting up crisis communication mechanisms.

Mapping the State of Implementation

Despite their growing adoption and widely recognised importance, research on how states actually implement multilateral cyber CBMs remains limited – particularly regarding the practical steps taken to translate commitments into action. Comparative assessments across regional organisations are particularly limited. Yet developing comparative insights into how these measures are implemented is critical for enhancing transparency, informing future policymaking, and helping resource-constrained states navigate an increasingly fragmented landscape of cyber initiatives.

Mapping implementation reveals which measures are actively applied, which rely on implicit actions, and how national, regional, and global practices interact. It also helps pinpoint gaps, best practices, and enabling factors that can guide future cyber CBM design and foster cross-regional cooperation. Responding to this gap, this paper systematically maps state practice in multilateral cyber CBM implementation across several organisations:

- Organization for Security and Co-operation in Europe (OSCE)
- Organization of American States (OAS)
- ASEAN Regional Forum (ARF)
- United Nations (UN)
- Economic Community of West African States (ECOWAS)
- Conference on Interaction and Confidence Building Measures in Asia (CICA)

The analysis focuses on those organisations that have explicitly adopted cyber CBMs and assesses the extent to which political commitments have been translated into practice through concrete actions. Implementation is described based on observable state practice, using different levels of progress.

To provide a balanced picture, the analysis takes into account explicit implementation, where actions are directly linked to specific cyber CBMs (e.g., nominating national PoCs), and implicit implementation, where broader national initiatives indirectly support cyber CBM objectives (e.g., developing strategies or capacity-building programmes). Recognising both modes avoids overstating success while still capturing practical contributions that enhance confidence and enable cyber CBM implementation.

Key Takeaways

- **Formulation is easier than implementation:** From the outset, the drafting process emphasised finding language that could secure consensus among states, leaving implementation details to later.
- **Capacity-building is foundational:** A lot of cyber CBM activities either aim to build up capacities or are connected to capacity-building measures as capacity itself is a prerequisite for successful implementation.
- **CBMs often work best as interconnected systems:** Some cyber CBMs have limited utility alone; taken together with other cyber CBMs, they form a coherent framework or lay the groundwork for more substantive cooperation.
- **Explicit deliverables enable measurability:** Cyber CBMs asking for concrete outputs (e.g., nomination of PoCs) are easier to monitor, with progress often published by regional secretariats. In contrast, information on other cyber CBMs is not publicly known, or it is more difficult to identify, especially if the implementation is mostly implicit.
- **Dialogue itself is a core outcome**: Beyond measurable outputs, the process of engagement, information exchange, and experience-sharing itself fosters trust and confidence. For some cyber CBMs, this is an explicit objective; for others, it emerges as a valuable by-product.
- **Success should not be measured by explicit outputs alone:** Cyber CBMs' value lies not only in tangible deliverables of individual cyber CBMs but also in the broader framework of communication and trust they create all together, particularly during geopolitical tensions.
- **Implementation is a continuous process:** Regions across the world increasingly view cyber CBMs as a valuable diplomatic tool with many committing to their adoption and implementation. However, implementation remains a work in progress – while some measures are being actively applied, others are still at early stages, and much remains to be done. Even well-established CBMs require sustained engagement, political will, and at times more ambitious interpretation to deepen their impact.
- **No one-size-fits-all model:** Regional implementation approaches vary regarding how organisations implement cyber CBMs but also to what they prioritise depending on institutional structures, mandates, and resources as well as the broader regional context.
- **Cross-regional exchange enhances progress:** Sharing experiences among regions strengthens mutual learning and fosters convergence around foundational cyber CBMs (like PoC directories and national strategy sharing).

2. Introduction: Why trust matters in the cyber domain

Trust is a cornerstone of any relationship – whether in society, economy, politics – and is equally vital in diplomacy.[1] Yet global politics is currently marked by diverse challenges; conflicts, growing competition, and an overall lack of trust. From Russia's war against Ukraine bringing back conflict to European soil[2] to China's strategic global ambitions connected to increasing militarisation[3] to growing unpredictability in United States foreign policy,[4] to violent conflicts across Africa, the Middle East, and South Asia, there is a growing lack of trust in international relations.[5] All of this also applies in the cyber domain – arguably mistrust plays an even stronger role here than in other areas.

This is partly because the cyber domain is extremely vulnerable to misunderstandings and miscalculations, exacerbated by various **structural and organisational aspects**: States may outsource operations to third parties, such as cyber mercenaries, maintaining plausible deniability.[6] The involvement of both state and non-state actors – including intelligence services, criminal networks, and hacktivists – adds layers of ambiguity,[7] making it difficult to determine the origin and intent of a cyber operation.[8] This complicates attribution, often turning it into a lengthy and complex process.[9]

States also frequently test offensive capabilities below the threshold of an armed attack, sometimes embedding them in adversary systems well before open conflict.

[1] McDonald, Scott (2022): Foreword. In: Trust in international relations, public diplomacy and soft power. A review of literature and data. British Council.

[2] Lehne, Stefan (2023): After Russia's War Against Ukraine: What Kind of World Order?. Carnegie Europe.

[3] Council on Foreign Relations (n.d.): China's Approach to Global Governance.

[4] Glasser, Susan (2025): Uncertainty is Trump's Brand. But what if he already told us exactly what he's going to do?. New Yorker.

[5] McDonald, Scott (2022): Foreword. In: Trust in international relations, public diplomacy and soft power. A review of literature and data. British Council.

[6] Lewis, James (2010): Multilateral Agreements to Constrain Cyberconflict. Arms Control Today.

[7] Bussolati, Nicolo (2015): The Rise of Non-State Actors in Cyberwarfare. In: Ohlin, Jens, Govern, Kevin, Finkelstein, Clair (Eds.), Cyberwar: Law and Ethics for Virtual Conflicts. Oxford University Press.

[8] Arimatsu, Louise (2012): A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations. In: Czosseck, Christian, Ottis, Rain & Ziolkowski , Katharina(Eds.), 4th International Conference on Cyber Conflict. NATO CCDCOE Publications.

[9] Kwiatkowski, Ivan, Kazakova, Anastasiya, Ryng, Julia, Chan, Kendrick (2022): 'Unpacking' technical attribution and challenges for ensuring stability in cyberspace.

However, such prepositioning is hard to differentiate from espionage. This can lead to unintended escalation, as decision-makers may misjudge the actions and intentions of other states.[10] In many cases, states refrain from clarifying suspected activities – either because they lack the technical capability for reliable attribution or choose to avoid public attribution for political reasons – further fuelling uncertainty and mistrust.[11]

Technical aspects add another dimension of uncertainty: Features such as obfuscation, anti-forensic features of malware or layers of intermediate command-and-control infrastructure allow operations to be conducted covertly, with perpetrators often able to manipulate or obscure digital traces to avoid identification.[12] This also enables false flag operations – where one actor deliberately imitates another[13] – or "fourth-party collection," in which an uninvolved threat actor exploits another's attack infrastructure (see examples for such operations in Annex I).[14] False flags, through tactics like foreign language markers, code reuse, creation of fake personas or hijacked infrastructure, can significantly delay or distort attribution.[15]

Another critical risk comes from uncontrolled malware propagation. Wormable or autonomous malware can spread far beyond intended targets (see examples for such operations in Annex I), causing collateral damage and escalating tensions especially when deployed in politically sensitive contexts and attribution remains unclear. Finally, because the cyber domain is borderless and interconnected, threats are inherently transnational,[16] with a single incident under certain conditions capable of cascading across borders and sectors.[17]

[10] Clapper, James (2015) in "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record, Senate Armed Services Committee.

[11] Brunner, Isabella (2022): The Prospects for an International Attribution Mechanism for Cyber Operations – An Analysis of Existing Approaches.

[12] Reinhold, Thomas (2020): Cyberspace as Military Domain: Monitoring Cyberweapons. In: Feldner, Denise (Ed.): Redesigning Organizations. Concepts for the Connected Society. Springer VS.

[13] Pihelgas, Mauno (2015): Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks. Tallinn: NATO CCDCOE.

[14] Guerrero-Saade, Juan, and Raiu, Costin (2017): Walking in Your Enemy's Shadow: When Fourth-Party Collection Becomes Attribution Hell.

[15] However, none of such operations have actually led to a conflict escalation.

[16] Radicevis, Velimir (2017): Promoting Cyber Stability between States: OSCE Efforts to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies (ICTs) in the Context of Global and Regional Security. In: IFSH: OSCE Yearbook.

[17] Gomez, Miguel Alberto and Winger, Gregory H. (2024): Third-party countries in cyber conflict: Public opinion and conflict spillover in cyberspace. Journal of Peace Research.

As the Netherlands, which is also part of an open, informal, cross-regional group aiming to advance CBMs, stressed in a 2022 statement during UN negotiations on cyber issues: “Under the current circumstances, the international community faces unprecedented risks of misinterpretation, miscalculation and escalation of cyber incidents.“[18] In such an environment, mechanisms for building and sustaining trust become especially urgent. To mitigate the risks, states have turned to multilateral measures that enhance predictability, transparency, communication, and cooperation.

Over the past two decades, the field of cyber diplomacy has evolved and established a framework to advance stability and cooperation in the cyber domain. Among the instruments are measures aimed at enhancing trust between states – known as cyber Confidence-Building Measures[19] (CBMs). Cyber CBMs are negotiated and implemented in unilateral, bilateral, and multilateral formats. Different multilateral organisations have developed and implemented multilateral cyber CBMs:

- the Organization for Security and Co-operation in Europe (OSCE) (since 2012[20]),
- the Organization of American States (OAS) (since 2017[21]),
- the ASEAN Regional Forum (ARF) (since 2015[22], implementation starting in 2018),
- the United Nations (UN) (since 2023[23]),
- the Economic Community of West African States (ECOWAS) (since 2024[24]),
- as well as the multilateral forum Conference on Interaction and Confidence Building Measures in Asia (CICA) (since 2021[25]).

[18] Netherlands Representative (2022): (7th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Second Substantive Session (28 March-1 April 2022).

[19] For the sake of consistency, this paper uses the term cyber CBMs, even though the OSCE, for example, uses the term cyber/ICT security CBMs. You will find a detailed definition of CBMs, and specifically cyber CBMs, in the following chapter.

[20] OSCE (2012): Permanent Council Decision No. 1039. Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.

[21] OAS CICTE (2017): CICTE/RES.1/17. Establishment of a Working Group on Cooperation and Confidence-Building Measures in Cyberspace.

[22] ARF (2015): ASEAN Regional Forum Working Plan on Security of and in the use of information and communications technologies (ICTs).

[23] Annex A of the second APR - UN General Assembly (2023): Developments in the field of information and telecommunications in the context of international security. (A/78/265).

[24] ECOWAS (2024): Directive C/DIR.2/12/12 on Cyber/ICT Confidence Building Measures.

[25] Find them here.

Despite their widely recognised importance and their growing adoption, research on their implementation remains limited – particularly regarding how states translate multilateral cyber CBMs into practice. Comparative assessments across multilateral organisations are especially scarce.[26] Yet developing systematic and comparative insights into how – and whether – these measures are implemented is critical for enhancing accountability and transparency in existing arrangements, informing policymaking on future initiatives, and helping resource-constrained states navigate an increasingly fragmented landscape of cyber initiatives.[27] Responding to this gap, this paper maps the current state of implementation of cyber CBMs within multilateral organisations.

The analysis begins by defining cyber CBMs, before introducing the key multilateral organisations engaged in this field. Drawing on document analysis and expert interviews, it then maps the implementation practice within these organisations (OSCE, OAS, ARF, UN, ECOWAS, CICA), presented in the order in which they first began implementing cyber CBMs.

[26] This need has also been highlighted by South Africa - specifically regarding CBMs - in the session on CBMs at the OEWG in 2023: "(...) given the fact that so many delegations have referred to CBMs used in regional organizations, it might be useful for us to consolidate a list of these for background information." (cf. South Africa's Representative (2023): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Fourth Substantive Session (6-10 March 2023).)

[27] Lewis, James (2025): The Practice of Cyberdiplomacy. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James (Eds.): A Handbook for the Practice of Cyber Diplomacy. EU Institute for Security Studies.

3. How to build trust

3.1. Confidence-Building Measures (CBMs)

CBMs have become known as a tool of international politics to mitigate East-West tensions during the Cold War.[28] One of the most well-known examples from this period was the "hot line" between Moscow and Washington, a direct line of communication between the head of government of nuclear-weapons states as part of efforts to reduce the risk that an accident, miscalculation, or surprise attack could trigger a nuclear war.[29] Within the context of the East-West détente, the Helsinki Final Act was signed at the 1975 Conference on Security and Cooperation in Europe, formally codifying CBM objectives for the first time. The Act described CBMs as an instrument "to contribute to reducing the dangers of armed conflict and of misunderstanding or miscalculation of military activities which could give rise to apprehension, particularly in a situation where states lack clear and timely information about the nature of such activities."[30]

While definitions of CBMs may vary across sources, their fundamental purpose remains the same: reducing (deep-seated) suspicions, concerns, and fears through increased confidence.[31] The "ultimate goal of confidence-building measures is to strengthen international peace and security and to contribute to the prevention of all wars."[32] As such, CBMs are structured agreements negotiated and implemented between states as a mechanism for crisis prevention, crisis management, and stability assurance.[33] They are voluntary and not legally binding,[34] but they

[28] Holst, Johan Jorgen (1983): Confidence-building Measures: A Conceptual Framework. In: Survival 25 (1), pp. 2–15.

[29] Memorandum of Understanding Between The United States of America and The Union of Soviet Socialist Republics Regarding the Establishment of a Direct Communications Link (1963).

[30] Conference on Security and Co-operation in Europe (1975): Helsinki Final Act.

[31] Ghernaouti, Solange and Crespo, Laura (2017): Building Confidence in the Cyber Realm as a Means of Preventing Conflict - a Swiss Perspective. In: European Cyber Security Journal 3 (1), pp. 10-25.

[32] United Nations General Assembly (1996): A compilation of all texts of principles, guidelines or recommendations on subject items adopted unanimously by the Disarmament Commission. Note by the Secretary-General (A/51/182).

[33] Healey, Jason, Mallery, John C., Jordan, Klara Tothova, Youd, Nathaniel V. (2014): Confidence-Building Measures in Cyberspace. A Multistakeholder Approach for Stability and Security.

[34] United Nations General Assembly (1996): A compilation of all texts of principles, guidelines or recommendations on subject items adopted unanimously by the Disarmament Commission. Note by the Secretary-General (A/51/182).

are politically binding.[35] States often honor them because public or diplomatic commitments carry weight: failing to do so can harm a state's reputation, erode trust, and strain relations.[36]

While CBMs cannot prevent intentional conflicts and wars, they can contribute to preventing unintentional conflicts "by stopping or slowing the spiral of escalation."[37] In practice, they can prevent escalation, support negotiations, and consolidate peace processes. Thus, they are not solutions in themselves, but function as crucial entry points or supporting measures within broader efforts to build peace and stability. Because of their trust-building function, CBMs help create a political environment more conducive to binding agreements[38] and often served as a stepping stone toward arms control and disarmament.[39] Their significance also extends far beyond the Cold War era and their initial military focus to include humanitarian, political, economic, environmental, societal, and cultural dimensions (see examples of these different kinds of CBMs in the Annex II).[40] To be effective, however, they must always be tailored to the specific context in which they are applied.[41]

3.2. A two-step process: Implementing CBMs

The process of establishing CBMs – like most policy processes – can be roughly divided into two steps:

[35] Zielkowski, Katharina (2013): Confidence Building Measures for Cyberspace. In: Katharina Zielkowski (Ed.): Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy.

[36] Schachter, Oscar (1977): The Twilight Existence of Nonbinding International Agreements. In: American Journal of International Law 71 (2), p.-296-304.

[37] Ott, Nikolas, and Osula, Anna-Maria (2019): The Rise of the Regionals: How Regional Organisations Contribute to International Cyber Stability Negotiations at the United Nations Level. In: 2019 11th International Conference on Cyber Conflict.

[38] Scherbak, Igor (1991): Confidence-building Measures and International Security. The Political and Military Aspects: a Soviet Approach. UNIDIR.

[39] Holst, Johan Jorgen and Melander, Karen Alette (1977): European security and confidence-building measures. In: Survival 19 (4), pp. 146-154.

[40] Mason, Simon J. A. and Siegfried, Matthias (2013): Confidence Building Measures (CBMs) in Peace Processes. In: Managing Peace Processes. Process related questions. A handbook for AU practitioners, pp. 57-77. // OSCE (2012): OSCE Guide on Non-military Confidence-Building Measures (CBMs).

[41] United Nations General Assembly (1996): A compilation of all texts of principles, guidelines or recommendations on subject items adopted unanimously by the Disarmament Commission. Note by the Secretary-General (A/51/182).

- **Formulation:** CBM formulation refers to “formal arrangements”[42] that specify “a series of actions that are negotiated [and] agreed” between states.[43] In other words, CBM formulation refers to words on paper. These agreements are typically formulated by consensus among all involved parties and adapted to specific contexts. In this first step CBMs may not go beyond statements of intent.
- **Implementation:** For CBMs to have any effect, they must be followed by actions in line with the formulated commitments.[44] CBM implementation refers to putting these words on paper “in practice,”[45] that is, “to take the actions required by the agreements.”[46] Implementation is not binary but rather can be described as an ongoing process of practices. Thus, “[t]he seriousness, credibility and reliability of a State‘s commitment to confidence-building can be demonstrated only by consistent implementation over time.”[47]

CBMs’ effectiveness depends on the latter – without tangible action, they remain largely theoretical.[48] Most CBMs are implemented through activities that can be summarized under the following objectives:[49]

[42] Bzostek, Rachel and Rogers, Allison (2014): Oslo +20: Reassessing the role of confidence building measures. In: The Social Science Journal 51 (2), pp. 250-259.

[43] Mason, Simon J. A., and Siegfried, Matthias (2013): Confidence Building Measures (CBMs) in Peace Processes. In: Managing Peace Processes. Process related questions. A handbook for AU practitioners, pp. 57-77.

[44] Mason, Simon J. A., and Siegfried, Matthias (2013): Confidence Building Measures (CBMs) in Peace Processes. In: Managing Peace Processes. Process related questions. A handbook for AU practitioners, pp. 57-77. // Holst, Johan Jorgen and Melander, Karen Alette (1977): European security and confidence-building measures. In: Survival 19 (4), pp. 146-154.

[45] Levite, Ariel E. and Landau, Emily B. (1997): Confidence and security building measures in the Middle East. In: Journal of Strategic Studies 20 (1), pp. 143-171.

[46] Bzostek, Rachel and Rogers, Allison (2014): Oslo +20: Reassessing the role of confidence building measures. In: The Social Science Journal 51 (2), pp. 250-259.

[47] United Nations General Assembly (1996): A compilation of all texts of principles, guidelines or recommendations on subject items adopted unanimously by the Disarmament Commission. Note by the Secretary-General (A/51/182).

[48] Toth, Szilvia (2025): Regional Organisations and Confidence-Building Measures. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James (Eds.): A Handbook for the Practice of Cyber Diplomacy. EU Institute for Security Studies.

[49] Holst, Johan Jorgen (1983): Confidence-building Measures: A Conceptual Framework. In: Survival 25 (1), pp. 2-15.

- **Information-sharing**: for example, exchanging data on (military) capabilities, expenditures, strategic doctrines, legal interpretations, and organisational structures.
- **Notification**: for example, providing advance notice of significant troop movements or establishing communication networks.
- **Observation**: for example, conducting inspections on the territory of other participating states, observing military exercises, or carrying out observation flights.
- **Stabilization**: for example, implementing measures to limit military activities and maintain military balance (this proves to be the most difficult category to negotiate).

To achieve CBMs' potential, regular assessment of their implementation is essential.[50] Drawing from comparison, some measures formulated as CBMs contain clearly defined objectives – akin to KPIs or deliverables – while others are more general, leaving room for varied interpretation. This variation underscores the importance of paying attention to two modes of implementation – often running in parallel:

- **Explicit implementation**: Some actions are clearly linked to a CBM – sometimes even verifiable – and explicitly designed to achieve its objective – for example, nominating a national PoC or sharing incident information through channels established under a CBM.
- **Implicit implementation**: In other cases, activities contribute to CBM objectives only implicitly, as part of broader policy priorities of the respective state. A state may, for instance, develop a national cybersecurity strategy, adopt an incident severity scale to enhance resilience, or fund capacity-building programs on gender equality primarily for domestic reasons; such actions support CBM purposes or enable implementation but are not formally presented as CBM-related.

Not every activity aligned with CBM objectives should automatically be counted as CBM implementation – doing so would overstate their impact and distort the picture. Nevertheless, recognising such implicit contributions is essential for understanding the broader environment in which CBMs operate. Capturing both explicit and implicit actions, therefore, enables a balanced picture. It avoids inflating success but still acknowledges the practical measures that, while not

[50] Ghernaouti, Solange and Crespo, Laura (2017): Building Confidence in the Cyber Realm as a Means of Preventing Conflict - a Swiss Perspective. In: European Cyber Security Journal 3 (1), pp. 10-25.

formally labelled as CBM implementation, strengthen confidence and help achieve the agreed objectives. Additional verifiability of states' activities to implement CBMs, where applied, further strengthens credibility by demonstrating whether commitments are being implemented. However, most CBMs are not designed to be verified or may only become verifiable at later stages.[51]

3.3. Why building trust in the cyber domain is challenging

As noted in the introduction, the risks of unintended escalation are even higher in the cyber domain than in other areas, due to its unique technical as well as structural and organisational characteristics. In response, CBMs have increasingly been extended to the cyber domain and tailored to its context.

The OSCE describes cyber CBMs as "practical measures which address misperceptions and misunderstandings in cyberspace," while the UN Group of Governmental Experts (GGE) defines them as "[c]onfidence-building, stability and risk reduction measures to address the implications of State use of ICTs." Similarly, the OAS emphasises their goal of achieving "a common understanding of acceptable State behavior in cyberspace, and a state of cyber stability in international relations." Taken together, these definitions from some of the relevant organisations analysed in this paper affirm that cyber CBMs are intended to strengthen trust, predictability, and mutual understanding among states, consistent with the overarching objectives of CBMs outlined above.

While traditional CBMs – such as those developed during the Cold War – also emphasised transparency, information exchange, and (military-to-military) communication, they often build on verification mechanisms.[52] In contrast, verification is especially difficult in the cyber domain.

To illustrate, consider inspections – a classic measure of verification. These can be conducted on-site or remotely using flyovers, photographs, or satellite imagery to assess the capacities of other states. Regarding the cyber domain, however, inspections are often deemed unfeasible for several reasons: A frequently cited challenge is that cyber capabilities cannot be numerically defined in the same way

[51] Holst, Johan Jorgen (1983): Confidence-building Measures: A Conceptual Framework. In:Survival 25 (1), pp. 2-15.

[52] Holst, Johan Jorgen (1983): Confidence-building Measures: A Conceptual Framework. In: Survival 25 (1), pp. 2-15.

as conventional armaments in the context of traditional CBMs. Malware can be copied, deployed globally within seconds, and lacks the noticeable physicality of tanks or missiles – besides their existence as data in clouds, on data carriers, or computers.[53]

Another often discussed challenge in this regard is the lack of a clear definition of what could be considered a 'cyberweapon' to ascertain the size of a state's cyber arsenal.[54] Effective verification via inspections – which would verify at least what makes a part of a state's cyber capabilities[55] like the bandwidth of malware or the stockpile of zero-day vulnerabilities – would require technical access to national systems. This is considered intrusive since it holds the risk of exposing sensitive vulnerabilities.[56] Much of the technical knowledge relevant to cyber operations can be used for different purposes: it can be applied for both defensive and offensive purposes, as well as for intelligence activities.[57] For example, the same exploit frameworks and vulnerability scanners that malicious actors use to identify and exploit weak systems are also indispensable for defenders conducting penetration testing to patch vulnerabilities and strengthen network resilience, or for intelligence services assessing exposure trends to anticipate threats and inform policy decisions. This overlap places it outside the scope of such agreements, but also renders it politically sensitive and therefore generally avoided in multilateral discussions.[58]

That said, parallels exist: states grant the International Atomic Energy Agency (IAEA) access for on-site inspections to secure nuclear facilities for verification,[59] illustrating both the sensitivity of such measures and the precedent for accepting them. Still, certain techniques render quantification in the context of inspections irrelevant altogether. A prominent example is living off the land (LOTL), a technique increasingly employed by Chinese threat actors.[60] Here, access might initially be gained through legitimate services like Windows Remote Desktop,

[53] Reinhold, Thomas and Reuter, Christian (2019): Verification in Cyberspace. In: Reuter, Christian (Ed.): Information Technology for Peace and Security.

[54] Pytlak, Allison (2024): Reimagining Cyber Arms Control.

[55] If capabilities is understood as "possessing the resources, skills, knowledge, operational concepts and procedures to be able to have an effect in cyberspace." (cf. Uren, Tom, Hogeveen, Bart, Hanson, Fergus (2018): Defining offensive cyber capabilities.)

[56] Denning, Dorothy (2001): Obstacles and Options for Cyber Arms Control. Heinrich Böll Foundation.

[57] Uren, Tom, Hogeveen, Bart, Hanson, Fergus (2018): Defining offensive cyber capabilities.

[58] Roguski, Przemyslaw (2021): An Inspection Regime for Cyber Weapons: A Challenge Too Far?

[59] Hibbs, Mark, Kuchinov, Vladimir, Rockwood, Laura, and Tuzov, Alexander (n.d.): IAEA Safeguards: Reaching Safeguards Conclusions.

[60] Joint Cybersecurity Advisory (2023): People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.

then the perpetrators exploit legitimate tools and features already present on a system – such as PowerShell or built-in administrative software. Thus, it depends more on human expertise than file-based malware and therefore cannot easily be detected through standard inspections.

Another traditional means of verification is the exchange of expenditure data. In conventional military contexts, such information has long served as an indicator of whether a state prioritises defensive or offensive capabilities.[61] In the cyber domain, however, spending is often considered a poor proxy due to several reasons: As Reinhold and Reuter note, "there is no obvious distinction for IT goods due to their dual-use character."[62] With few exceptions (such as in the context of Stuxnet, see Annex I), most tools that could be used offensively – like penetration testing software or vulnerability scanners – can also be used defensively or for intelligence purposes, which in turn would not be within the scope of such agreements. Additionally, most software used for these offensive and defensive purposes are also used in both civilian and military IT infrastructure. Accordingly, cyber budgets cannot be neatly divided into established categories such as military vs. civilian or offensive vs. defensive.

Still, expenditure data could potentially offer insights into the scope of cyber programs and possible trends. Cyber power rests more on human expertise than on material assets. Thus, in theory, a state's investments in personnel might provide valuable information about its capabilities.[63] This could become particularly meaningful when combined with knowledge of organisational structures, such as the establishment of dedicated military or intelligence cyber units. Skills like vulnerability discovery and reverse engineering are frequently linked to offensive operations, yet they are equally indispensable for defense[64] – underscoring the same dilemma. Nevertheless, information such as the types of expertise being recruited, especially in conjunction with information on the budget spent on contracts with offensive cyber companies, might help identify trends.[65] Especially considering that several states have explicitly referenced "offensive cyber capabilities" in recent national strategies.[66] Taken together, this suggests that

[61] Wezeman, Pieter, Béraud-Sudreau, Lucie, Marksteiner, Alexandra and Tian, Nan (2022): A Practical Guide to State Participation in the UN Report on Military Expenditures.

[62] Reinhold, Thomas and Reuter, Christian (2019): Verification in Cyberspace. In: Reuter, Christian (Ed.): Information Technology for Peace and Security.

[63] Uren, Tom, Hogeveen, Bart, Hanson, Fergus (2018): Defining offensive cyber capabilities.

[64] Mott, Gareth, Shires, James, Ellis, Jen, Sullivan, Jamens and MacColl, Jamie (2024): State Permissive Behaviours and Commercial Offensive-Cyber Proliferation.

[65] NCSC (2023): The threat from commercial cyber proliferation.

[66] Uren, Tom, Hogeveen, Bart, Hanson, Fergus (2018): Defining offensive cyber capabilities.

while expenditure-based verification or analysis in the cyber domain would remain complex and insufficient on its own, it could still hold some analytical value when considered with other sources of information.

Although verification challenges have been discussed for more than two decades – particularly in the context of arms control discussions in the cyber domain – debates have often fallen short of capturing the nature of current threats and developments, underscoring why further research into cyber verification remains essential. To date, cyber CBMs have been adopted without dedicated verification mechanisms, likely reflecting both the absence of practical methods and a lack of political will to pursue them. Instead, cyber CBMs focus on reducing the risks of miscalculation through voluntary information sharing, transparency, and cooperation.

As instruments of international politics, such cyber CBMs are negotiated and implemented between states in unilateral,[67] bilateral,[68] and multilateral forms.

[67] A common unilateral cyber CBM is the publication of a state's position on how international law applies in cyberspace. An increasing number of states are releasing such statements, helping to advance the global discussion and build a shared understanding. These measures enhance transparency and predictability in state behavior. Germany, for instance, published its position in 2021.

[68] Bilateral agreements for example existed between the United States and Russia until the Russian invasion of Ukraine in 2014. The two states created a working group on CBMs that developed a set of measures to enhance transparency and to reduce instability as well as the risk of escalation due to misunderstandings. These measures included establishing different lines of communication to enable the exchange of information regarding ICT security, e.g. via the CERTs of the two states, the Nuclear Risk Reduction Center (NRRC), and a direct voice communication line between the United States. Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council so that they could directly manage a crisis emerging from an ICT security incident (see here). Another well-known example of bilateral cyber CBMs is an agreement from 2015 between China and the United States addressing cybercrime activities, in particular cyber espionage. The agreement included communication measures, e.g. timely response to provide requested information and cooperation measures in the shape of assistance in the case of malicious cyber activities (see here). However, bilateral CBMs are typically confidential - this secrecy can create dynamics of trust among involved parties but also breed suspicion among excluded states (cf. Pawlak, Patryk (2016): Confidence-Building Measures in Cyberspace: Current Debates and Trends. In: Anna-Maria Osula, Henry Rõigas (Eds.): International cyber norms. Legal, policy & industry perspectives. NATO Cooperative Cyber Defence Centre of Excellence.).

In addition, there are numerous initiatives of cooperation between different states for instance to build capacity,[69] (informal) regional networks,[70] dialogue platforms, diplomatic 1.5/2.0 dialogues, or workstreams within regional organisations and fora focusing on cybersecurity[71] which also contribute to building confidence and to the overall objectives of CBMs.

Among these, multilateral cyber CBMs within regional organisations often have the most sustainable and wide-reaching impact due to various reasons:[72] Regional approaches account for different levels of cyber maturity and distinct (geo)political priorities shaped by culture, history and structure. Compared to universal fora – such as Open-ended Working Groups (2019-2021, 2021-2025) and the outcomes of the UN Group of Governmental Experts, which were adopted by the General Assembly – regional initiatives can deliver more agile, targeted, and practical solutions among states with shared interests and experiences.[73] They also tend to maintain closer relations with national authorities, allowing them to better understand and reflect national perspectives.[74] Member states of a regional organisation often share similar threat perceptions and are, therefore, well positioned to address common challenges. On the other hand, regional organisations also bring together states with strained relations – neighbours that may be directly affected by each other's actions or suspicions of malicious

[69] Joint initiatives focusing on capacity-building like the AU's African Cyber Capacity Building Framework, the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), efforts within the EU's cyber capacity building network and within the International Telecommunication Union (ITU), as well as countless multilateral project based initiatives between partnering states contribute to enhancing cooperation and thereby build trust. Fellowships like the Women in Cyber Fellowship or HerCyber Track also contribute to building trust between its participants, moreover, the adoption of a shared position on international law by the African Union (AU) promotes transparency and predictability.

[70] Networks like the Forum of Incident Response and Security Teams (FIRST), the Pacific Cyber Security Operational Network (PaCSON), and the Western Balkan Cyber Diplomacy Network, as well as the Smart Africa Secretariat's efforts to establish and operationalise National and Regional CSIRTs across African Union (AU) member states, the European Union Agency for Cybersecurity (ENISA), and an ASEAN Regional CERT contribute to building avenues for information exchange and trust.

[71] Dialogue platforms like the annual ASEAN Ministerial Conference on Cybersecurity (AMCC), the Council of Arab Ministers of Cybersecurity, the the BRICS Working Group on Cybersecurity, the Shanghai Cooperation Organization, G7 dialogue on cybersecurity, diplomatic 1.5/2.0-track dialogues like the Sino-European Cyber Dialogue, initiatives like the Pall Mall Process, numerous public-private partnership initiatives as well as countless joint conferences and workshops create spaces for information sharing, exchange and encounter and thereby contribute to building confidence.

[72] Pawlak, Patryk (2016): Confidence-Building Measures in Cyberspace: Current Debates and Trends. In: Anna-Maria Osula and Rõigas, Henry (Eds.): International cyber norms. Legal, policy & industry perspectives. NATO Cooperative Cyber Defence Centre of Excellence.

[73] UNIDIR (2019): The Role of Regional Organizations in Strengthening Cybersecurity and Stability: Experiences and Opportunities Report of the 2nd International Security Cyber Workshop Series.

[74] Greminger, Thomas (2019): Opening Remarks.

activity – and thus serve as important platforms for dialogue, risk reduction, and the prevention of misperception.[75] Moreover, regional organisations can build on established processes and initiatives, such as capacity-building activities and trusted communication channels.[76]

[75] Hiller, Ben (2019): OSCE Confidence Building Measures to reduce the Risks of Conflict Stemming from the Use of ICTs.

[76] Ott, Nikolas, and Osula, Anna-Maria (2019): The Rise of the Regionals: How Regional Organisatiaons Contribute to International Cyber Stability Negotiations at the United Nations Level. In: 2019 11th International Conference on Cyber Conflict.

4. Where we stand today: The state of implementation of cyber CBMs

This analysis focuses on those multilateral organisations that have explicitly adopted cyber CBMs. It examines their implementation – that is, the extent to which commitments have been translated into practice through concrete actions. As the most tangible indicator of implementation, state practice serves as the main source of evidence.[77] Each cyber CBM is therefore analysed in two parts: first, its content and purpose are outlined; second, the current state of its implementation is described based on observed practice. To capture different degrees of progress, the following levels of implementation are used throughout the analysis:

- **not implemented:** The cyber CBM is (up till now) formulated but not followed by action.
- **implemented, but not widely:** The cyber CBM has seen some progress, with a limited number of states implementing it or engaging in related activities, but overall uptake remains rather low and gaps persist.
- **widely implemented:** The cyber CBM is actively implemented by a large majority of states and/or a large majority of states are participating in corresponding activities aiming at implementation.
- **no (sufficient) data available:** Too little information can be obtained or was publicly available to assess their implementation.

4.1. Organization of Security and Co-operation in Europe (OSCE)

4.1.1. Formulation of OSCE cyber CBMs

The Organization for Security and Co-operation in Europe (OSCE) is the world's largest regional security organization, established in 1975 to promote peace, democracy, and stability across Europe, North America, and Central Asia, with

[77] Such state practice can be tracked via media reporting, public government communications, as well as expert interviews.

57 participating states.[78] The OSCE, with its long history in traditional arms control, takes a comprehensive approach to security that extends beyond military and political issues to include economic, environmental, and human dimensions.[79]

In recent years, cybersecurity has become a growing area of focus due to the increasing threats posed by cyber incidents to national and regional stability.[80] In 2012 an open-ended Informal Working Group (IWG) was established and tasked with the "[d]evelopment of confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies."[81] Since then, the OSCE participating states established 16 cyber CBMs ("cyber/ICT security CBMs"), eleven of which were agreed on in 2013,[82] and five additional ones in 2016.[83] The first set of cyber CBMs describes transparency measures "which promote cyber resilience and preparedness, encourage communication and increase transparency."[84] Meanwhile, the second set defines co-operative measures; "which further address effective communication channels, public-private partnerships (PPPs), critical infrastructure protection and the sharing of vulnerability information."[85]

In 2017, it was decided not to adopt, for the time being, any additional cyber CBMs and instead focus efforts on implementing those already in place.[86] In parallel, the Adopt-a-CBM initiative was introduced in 2018 by the IWG chair,

[78] Albania, Andorra, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Holy See, Hungary, Iceland, Ireland, Italy, Kazakhstan, Kyrgyzstan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Mongolia, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Tajikistan, Turkey, Turkmenistan, Ukraine, United Kingdom, United States, and Uzbekistan.

[79] See more here.

[80] See more here.

[81] OSCE (2012): Permanent Council Decision No. 1039. Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.

[82] OSCE (2013): Permanent Council Decision No. 1106. Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.

[83] OSCE (2016): Permanent Council Decision No. 1202. OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.

[84] OSCE (2023): 10 Years of OSCE Cyber/ICT Security Confidence-Building Measures.

[85] OSCE (2023): 10 Years of OSCE Cyber/ICT Security Confidence-Building Measures.

[86] OSCE (2017): Ministerial Council Decision No 5/17. Enhancing OSCE Efforts to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.

inviting states or a group of states to champion the elaboration of modalities for implementing a specific cyber CBM.

The OSCE Secretariat's Transnational Threats Department (TNTD) supports participating states in implementing cyber CBMs at both the national and regional levels by organising capacity-building activities such as trainings, workshops, and technical briefings on topics ranging from cyber diplomacy to the protection of critical infrastructure and by fostering a community of national cyber experts to strengthen cooperation and resilience.[87]

4.1.2. Implementation of OSCE cyber CBMs

CBM 1

CBM 1 (2013): *"Participating States will voluntarily provide their national views on various aspects of national and transnational threats to and in the use of ICTs. The extent of such information will be determined by the providing Parties."*

Background: The aim of this CBM is to exchange information on national and transnational threats with ICTs. In doing so, this CBM fosters transparency and helps identify potential opportunities for cooperation between states.[88] This was a meaningful step forward at the time, given that even a voluntary exchange of national threat assessments was politically sensitive and required extensive negotiation, reflecting the broader challenges of building trust in the cyber domain.

Practice: Within the OSCE, national views on ICT-related threats are shared through three main channels. First, the internal POLIS Knowledge and Learning Platform allows states to share threat assessments with other participating states. Routine advisories posted there directly serve the goals of this CBM.[89] In line with CBM 1, participating states regularly release cybersecurity assessments and advisories, offering insights into evolving cyber threats and their potential impact on national security.[90] Second, and central to this CBM, the exchange of threat-related information has grown with the expanded use of the communication network established under CBM 10. While only a subset of participating states use it regularly, it provides a trusted channel for secure information sharing,

[87] OSCE (2023): 10 Years of OSCE Cyber/ICT Security Confidence-Building Measures.

[88] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[89] OSCE (2023): 10 Years of OSCE Cyber/ICT Security Confidence-Building Measures.

[90] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

particularly for distributing sensitive threat reports. Finally, the IWG meets several times a year (while CBM 11 stipulates at least three meetings annually, in practice four sessions are held each year), providing an important forum for in-person exchange of such information.[91]

Rather than create new structures or specific activities focusing explicitly on the implementation of this CBM, the OSCE focuses on leveraging these existing platforms to foster continuous, transparent information-sharing. With this in mind, it is hard to assess the explicit implementation of this CBM. Overall, however, this CBM is **implemented, but not widely**.

CBM 2

CBM 2 (2013): *"Participating States will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs."*

Background: Because cyber operations are transnational and technically complex, the timely exchange of threat information is indispensable for early detection, confident attribution, and collective action such as sanctions.[92] However, one key obstacle to such collaboration is trust: actors must be confident in the quality and intent behind the shared information.[93] This CBM calls on OSCE participating states to deepen voluntary cooperation and information-sharing among their national cybersecurity bodies such as CERTs, law-enforcement, regulators, and policy agencies so they can mount faster, better-coordinated responses to ICT threats. Thus, it promotes cyber resilience and readiness.[94]

Practice: In terms of explicit activities, there is **no sufficient data** to describe the implementation status of this CBM, partly due to its lower uptake within the Adopt-a-CBM initiative. However, in connection with CBM 4 and CBM 6, the OSCE regularly conducts regional and subregional exercises that simulate fictitious cyber incidents and require coordination among relevant national entities to formulate an effective response, serving both to test the robustness of national

[91] OSCE (2022): The OSCE Secretariat's intervention at the OEWG intersessional meeting.

[92] This has been exemplified in operations targeting the OPCW and the German Bundestag, in which attribution relied heavily on external partners, particularly the Five Eyes countries, such as the UK and the US. (Bendiek, Annegret and Schulze, Matthias (2021): Attribution: A Major Challenge for EU Cyber Sanctions. An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW. SWP Research Paper 11.)

[93] Pihelgas, Mauno (2015): Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks. Tallinn: NATO CCDCOE.

[94] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

cybersecurity mechanisms and to identify gaps and areas for improvement.[95] Moreover, the objective of this CBM is connected to most other CBMs and therefore implicitly to their implementation activities.

CBM 3

CBM 3 (2013): *"Participating States will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and on possible emergence of political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity."*

Background: This CBM is particularly relevant when a state detects a serious incident and suspects, based on limited information, another OSCE participant of involvement. In such cases, bilateral consultations are encouraged to enable early information-sharing, reduce misinterpretation, and build a fuller picture of events. This process may confirm or challenge initial assumptions,[96] while also offering a discreet diplomatic channel for states unwilling to publicly attribute an operation – whether to avoid exposing capabilities and vulnerabilities, or for political reasons. Through this mechanism, states can seek clarification, request harmful activity to stop, or ask for assistance.[97] In essence, the CBM provides a concrete procedure for information exchange during cyber incidents as a responsive crisis communication tool that lowers the risk of unintended escalation.[98]

Practice: The OSCE's existing crisis-management procedures, originally designed for conventional military activities, do not easily translate to the cyber domain. However, Germany and Switzerland, as CBM-adopters,[99] have prioritized advancing the implementation of this CBM as it is viewed as a core measure. Their initial focus was on developing clear procedures for requesting information and consultations in the event of an incident – a process that has since been completed. Although CBM 3 has not yet been applied in a real case, it was tested in a successful 2024 scenario-based tabletop exercise that combined it with other relevant CBMs, with all participating states engaging constructively. A follow-up exercise was executed in 2025. It was conducted in coordination with PoCs (CBM 8),

[95] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[96] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[97] Ben Hiller (2018): OSCE Experts: Cyber/ICT Security (Video Interview).

[98] Felix Kroll via OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[99] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

the communication network (CBM 10), and information-exchange templates (CBM 13), ensuring a more realistic starting point. With these procedures in place and tested, the CBM is now **widely implemented** and actively practiced through such exercises.

Overall, this CBM is closely linked to CBM 8, CBM 10, and CBM 13, together forming an interconnected framework offering a practical tool for managing international cyber incidents. This framework helps clarify key questions: who initiates which mechanism, and under what circumstances.[100] In addition, CBM 3 is connected to CBM 15: since 2021, the OSCE has launched extra-budgetary projects focusing on both CBMs, particularly on crisis communication, incident classification, and ICT crisis management.[101]

CBM 4

CBM 4 (2013): *"Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet."*

Background: This CBM invites OSCE participating states to voluntarily share information on national efforts to ensure an open, secure, interoperable, and reliable internet, which is an essential foundation for global connectivity, economic growth, and stability. While these terms are not always precisely defined, they generally refer to enabling users to access and exchange information freely, ensuring the internet functions as a neutral conduit for data, maintaining compatibility across systems, safeguarding data and infrastructure through strong security measures, and preserving functionality even amid disruptions. By exchanging such information, states enhance transparency while strengthening collective cyber resilience and readiness.[102]

Practice: Compared to other cyber CBMs, this measure is broadly formulated and best understood as both a commitment to the overarching objective and a framework for exchanging information and sharing best practices. A wide range of actions, which are regularly implemented by the participating states, can support this goal, including advocating for it in multilateral fora, integrating it into national cybersecurity strategies, enacting legal frameworks to protect

[100] Radicevis, Velimir (2017): Promoting Cyber Stability between States: OSCE Efforts to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies (ICTs) in the Context of Global and Regional Security. In: IFSH: OSCE Yearbook.

[101] OSCE (2022): Cyber Incident Classification. A Report on Emerging Practices within the OSCE region.

[102] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

digital rights, investing in secure infrastructure, or advancing efforts to counter cybercrime. In the OSCE's e-learning course on CBMs, Canada – one of the adopters alongside Kazakhstan[103] – showcased its Digital Charter and National Cyber Security Strategy as examples of transparent governance. Such measures illustrate the CBM's purpose: to facilitate the exchange of lessons learned, policy updates, and relevant developments, rather than to prescribe explicit measurable activities. IWG meetings provide a venue for such reporting.[104]

This CBM is closely connected to CBM 2 and CBM 6, as the OSCE regularly organises regional and subregional cybersecurity exercises under these frameworks to test national response capabilities, identify gaps, and foster continuous improvement. Given the wide disparities in cyber maturity among participating states, the measure provides important opportunities for capacity-building and peer learning.[105] To advance implementation, Canada and Kazakhstan developed a non-paper outlining steps to strengthen cyber cooperation.[106] In 2024, they also circulated a questionnaire to participating states to gather information on national efforts to promote an open, secure, interoperable, and reliable internet, with results expected to be shared at the IWG. While activities exist, explicit implementation efforts remain limited, so this CBM is **implemented, but not widely**.

CBM 5

CBM 5 (2013): *"The participating States will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats. The participating States will explore further developing the OSCE role in this regard."*

Background: This CBM designates the OSCE as a central forum where participating states exchange best practices, coordinate capacity-building programmes, and raise collective awareness on ICT security. The objective is to bolster regional cyber resilience while complementing (not duplicating) existing initiatives.

[103] Kazakhstan's Representative (2022): (7th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Second Substantive Session (28 March-1 April 2022).

[104] OSCE (2022): The OSCE Secretariat's intervention at the OEWG intersessional meeting.

[105] OSCE (2024): Statement by OSCE Secretariat at the intersessional meeting of the UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025.

[106] Kazakhstan's Representative (2022): (7th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Second Substantive Session (28 March-1 April 2022).

Practice: This CBM is also broadly framed and centers on information exchange as a means of promoting transparency and identifying opportunities for cooperation in the field of capacity-building. The POLIS Knowledge and Learning Platform plays a central role in supporting this exchange.

In the OSCE's e-learning course on cyber CBMs, the UK, one of its adopters, highlighted its work with over 100 countries and investments of over £36 million in CCB since 2012, including the development of national cyber strategies, law enforcement training, and public awareness campaigns.[107] These efforts illustrate the types of activities relevant to this CBM. However, it is important to note that not all CCB initiatives by OSCE states automatically count as implementation; rather, the CBM focusses on the sharing of information about such initiatives.

The OSCE also conducts capacity-building activities that contribute to this CBM being **widely implemented.** Through the project "Activities and Customized Support for the Implementation of OSCE Cyber/ICT Security Confidence-Building Measures," the organisation has delivered workshops on gender perspectives in cybersecurity,[108] cyber diplomacy,[109] norms, and the CBMs themselves,[110] alongside tabletop exercises testing their practical applicability. These efforts – implemented by the OSCE Secretariat's TNTD and regional missions, sometimes in cooperation with partners – naturally advance multiple CBMs at once. For example, a scenario-based discussion on responding to a major cyber incident linked this CBM to CBM 15. Such activities are funded by multiple states including Switzerland, the UK, and the Netherlands. A concrete illustration comes from Serbia, where the OSCE Mission supported initiatives ranging from awareness-raising and national strategy development to building effective communication channels, strengthening PPPs, and securing critical infrastructure.[111]

Finally, to enhance transparency and track implementation, the adopters distributed a questionnaire to participating states in 2024, with the results expected to be presented at the IWG.

[107] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[108] e.g., see here or here.

[109] e.g., see here, here, and here.

[110] e.g., see here.

[111] see here.

CBM 6

CBM 6 (2013): *"Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs. The OSCE participating States agree that the OSCE shall not duplicate the efforts of existing law enforcement channels."*

Background: Transnational cooperation is essential for detection, investigation, and prosecution, enabling timely information sharing, coordinated responses, and the harmonisation of legal frameworks to combat cybercrime.[112] This CBM encourages OSCE participating states to adopt national legislation that enables timely and voluntary cooperation between law enforcement and other relevant authorities in combating the criminal or terrorist use of ICTs. The goal is to strengthen cross-border cooperation by having clear legal pathways in place while avoiding duplication of existing mechanisms. It therefore describes steps to consider by states at the national level.[113] Measures may include streamlining legal frameworks for data sharing, harmonizing procedures for digital evidence exchange, and designating national contact points for urgent cybercrime-related cooperation.

Practice: This CBM is **widely implemented**, as the vast majority of OSCE participating states have legal frameworks in place to support cross-border cooperation against the criminal or terrorist use of ICTs. A key example is the Budapest Convention on Cybercrime, which entered into force in 2004 and has since been signed and/or ratified by 85% of OSCE states.[114] The convention establishes a legal basis for international cooperation through timely information

[112] Interpol (n.d.): When cybercriminals go global, our response must be international.

[113] Minárik, Tomáš (2016): OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection.

[114] The Budapest Convention on Cybercrime - established by the Council of Europe - is the first international legally binding treaty aimed at addressing cybercrime and electronic evidence,by harmonizing national laws, improving investigative techniques, and fostering international cooperation. Following this, 80 % of states worldwide used the Conventions for guidance or as a source for their domestic legislation. See here. OSCE participating states who are party to the Budapest Convention: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lichtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Moldova, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye, Ukraine, United Kingdom, United States; OSCE participating states who are signatories and invited to accede: Ireland, Kazakhstan.

sharing, mutual legal assistance, and expedited access to stored and traffic data.[115] Beyond this, all OSCE states are members of Interpol,[116] while EU member states also participate in Europol[117] and many non-EU OSCE members have formal cooperation agreements with Europol (covering another 85% of the OSCE, though Russia is currently suspended).[118] Since both organisations prioritise coordinated information exchange, these memberships further illustrate how legal and institutional mechanisms for cooperation exist across the region. More recently, in December 2024, the United Nations Convention against Cybercrime was adopted,[119] which will enter into force in the beginning of 2026 with 65 states having signed the treaty in October 2025.[120]

The annual C-PROC overview further highlights that legislative reform in this area is an ongoing global process. By December 2024, 95% of UN member states had reformed or were in the process of reforming legislation on cybercrime and electronic evidence. Taking a closer look at the regions with participating states within the OSCE, Europe was at 100%, the Americas at 97%, and Asia at 90%.[121] It is, however, important to stress that such efforts are not undertaken for the purpose of implementing this CBM. Rather, the CBM serves as an affirmation of these broader goals and provides a dedicated platform for dialogue.

[115] Council of Europe (2001): Convention on Cybercrime. European Treaty Series - No. 185.

[116] Interpol supports its member states by providing access to global police databases, investigative and forensic assistance, training, and coordination across key crime areas - such as terrorism, cybercrime, and organized crime - while facilitating international police cooperation, even between states without diplomatic ties, aiming to provide a politically neutral and legally respectful framework. See here.

[117] Europol supports EU member states' law enforcement by facilitating information exchange, providing analytical and technical assistance, producing strategic threat assessments, and promoting harmonized investigative methods through training and awareness-raising initiatives. See here. OSCE participating states who are also Europol member states: Austria, Belgium, Bulgaria, Croatia,Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

[118] See here - Operational Agreements with OSCE participating states, which allow for the exchange of information including personal data: Canada, Georgia, Moldova, Norway, Serbia, Lichtenstein, Ukraine, Albania, Bosnia and Herzegovina, Iceland, Montenegro, North Macedonia, Switzerland, Monaco, United States; Strategic Agreements with OSCE participating states, which allow for the exchange of information such as general intelligence or strategic and technical information, excluding personal data: Türkiye, Russia (suspended); Working Arrangements with OSCE participating states, which are similar to strategic agreements: Andorra, Armenia, San Marino; EU Agreements on Europol Cooperation/Adequacy Decisions with OSCE participating states: United Kingdom.

[119] The UN Convention against Cybercrime is the first comprehensive global treaty on this matter, which provides states with a range of measures to be undertaken to prevent and combat cybercrime, aiming to strengthen international cooperation in sharing electronic evidence for serious crimes. Find more information and the full text here.

[120] See here.

[121] Council of Europe (2025): The global state of cybercrime legislation 2013-2024: A cursory overview.

Each IWG meeting includes a standing agenda item for national updates, including legislative developments.[122] In addition, the OSCE conducts capacity-building activities that strengthen implementation, such as workshops linked to CBM 2 and CBM 4, as well as its "Regional Capacity-Building Project on Combating Cybercrime in Central Asia."[123] This multi-year project, launched in 2020 with support from Germany, the US, and other states, targets states that are neither signatories to the Budapest Convention nor members of Europol (Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan). Its activities focus on four pillars: strengthening training institutions, developing digital forensic capacity, enhancing regional cooperation, and raising awareness among policymakers and the public, all while embedding human rights considerations. A dedicated training guide on integrating human rights into daily criminal justice practice was also released.[124] By mid-2024, nearly 600 police officers and prosecutors from the region had received OSCE training, while law enforcement institutions were equipped with IT systems and educational materials to support cybercrime education. This project has also fostered new professional networks and partnerships, building on earlier workshops that addressed capacity gaps in the region.[125] Ultimately, effective international cooperation in combating cybercrime depends not only on legal frameworks but also on the capacity of states to put them into practice.

CBM 7

CBM 7 (2013): *"Participating States will voluntarily share information on their national organization; strategies; policies and programmes – including on cooperation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties."*

Background: This CBM encourages OSCE participating states to voluntarily exchange information on how they structure and govern national cybersecurity efforts, such as through strategies, policies, public-private partnerships (PPPs), and institutional frameworks. This is a quite traditional CBM, especially focused on building transparency, but it also acknowledges the crucial role of the private sector in enhancing cybersecurity.

[122] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[123] See here and here.

[124] Find it here.

[125] Examples are a workshop on "Strategic approaches to professional development on cybercrime and electronic evidence for law enforcement" in Tajikistan and a workshop to "develop strategic approaches to training on cybercrime and electronic evidence" in Kyrgyzstan.

Practice: This CBM, like so many others, thrives on regular exchange. There are two main options for exchanging information to implement this CBM: documents can be exchanged via the POLIS Knowledge and Learning Platform.[126] In 2019, more than 200 documents from numerous OSCE participating states were already available there. However, the use of the platform has declined somewhat in recent years. States also regularly use IWG meetings to share updates on this topic. In addition, states publish such documents via channels like their own websites or the UNIDIR Cyber Policy Portal. Furthermore, this CBM is connected to others; for example, CBM 14 also aims to facilitate the exchange of best practices regarding PPPs. Overall, the CBM is **widely implemented**.[127]

CBM 8

CBM 8 (2013): *"Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level."*

Background: This CBM establishes a network of designated national Points of Contact (PoCs) to facilitate communication between participating states on matters of cyber/ICT security, including during incidents. Its purpose is to enable rapid coordination, reduce response times, and minimise the risk of misinterpretation or escalation by ensuring that relevant authorities – both technical and political – can reach each other. Establishing a PoC-network was also a crucial CBM in the past as well as in other domains. Some regard it as the most critical CBM of all, as it underpins the effective functioning of the other CBMs and represents a fundamental objective of the confidence-building process.[128] Together with CBM 3, CBM 10, and CBM 13, it constitutes a central element of the OSCE's cyber crisis communication mechanism.

[126] OSCE (2024): Statement by OSCE Secretariat at the intersessional meeting of the UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025.

[127] OSCE (2022): The OSCE Secretariat's intervention at the OEWG intersessional meeting.

[128] e.g., Sziliva Tóth in 2023 on the "Inside Cyber Diplomacy"-Podcast by James Lewis and Christopher Painter in the episode "Implementing Cyber Confidence-Building Measures".

Practice: This CBM is among the best-known and most **widely implemented**. While only around 60% of participating states had nominated PoCs in 2015, today all but one participating state have voluntarily shared at least one PoC, typically comprising technical contacts from CERTs/CSIRTs and policy contacts from Ministries of Foreign Affairs.[129]

This success is largely the result of sustained outreach and capacity-building efforts by the OSCE Secretariat's TNTD. For instance, the project "Strengthening the Work of the CBM 8 Points of Contact Crisis Communication Network", supported over the years by the Netherlands, Germany, the US, and other states, has fostered bilateral visits (also of non-like-minded states), study tours, online events, and practical engagement among PoCs.[130] Since 2019, annual PoC conferences and expert online sessions have further ensured that these contacts are more than names in a database, helping to build a genuine community of trust.[131] Moreover, every workshop and each IWG meeting under CBM 11 contributes to sustaining this network, strengthening the familiarity and relationships that are critical for effective crisis communication.

Participating states are required to update PoC information within 30 days of any changes. The OSCE Secretariat's TNTD manages the contact data via the POLIS platform, which also hosts a dedicated cyber/ICT security workspace. To maintain reliability, the OSCE conducts biannual Communication Checks (CommsChecks), a practice initiated in 2016 and continually refined. These exercises test responsiveness and coordination, ranging from verifying contact details (with confirmation required within 24 hours) to addressing complex, cross-border incident scenarios within 48 hours, using both the POLIS platform and information-exchange templates under CBM 13. Shared information in these processes are often linked to CBM 1 or CBM 15, and exercises also encourage inter-agency and cross-national coordination. The OSCE Secretariat's TNTD monitors implementation and provides anonymised reports on CommsCheck performance, such as participation and response times, during IWG meetings and in reports to states.[132] There is a good response rate overall.

While the Secretariat does not track the actual use of the PoC directory, some states have publicly shared their experiences, including within UN discussions related to the Global PoC Directory (UN CBM 1). For example, Kazakhstan

[129] OSCE (2022): The OSCE Secretariat's intervention at the OEWG intersessional meeting.

[130] Find examples for such a study visit here and here, more about the project here.

[131] OSCE (2024): OSCE holds fourth annual meeting of national cybersecurity points of contact in Vienna.

[132] OSCE (2022): The OSCE Secretariat's intervention at the OEWG intersessional meeting.

requested information from another state via the PoC network during a cyber incident,[133] the Czech Republic used the network during the COVID-19 pandemic to warn OSCE partners of malicious cyber activities on hospitals,[134] and Germany has actively used the network since May 2022 to share information on major incidents amid heightened geopolitical tensions, including the 2023 cyber operation on municipal IT service provider Südwestfalen-IT (SIT) in North Rhine-Westphalia.[135]

CBM 9

CBM 9 (2013): *"In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating States will, as a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. Each participating State will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating States will endeavour to produce a consensus glossary."*

Background: This CBM seeks to reduce the risk of misunderstanding among participating states by fostering transparency around key cybersecurity-related terms. Since states often apply different definitions to relevant concepts, this measure encourages them to voluntarily share their national terminology and definitions. Doing so helps establish a clearer, common understanding, an especially critical asset during times of crisis. Over time, such exchanges are intended to contribute to the development of a shared, consensus-based glossary, thereby enabling more precise dialogue and more effective cooperation in the field of cybersecurity.

Practice: This CBM can be broken down into two phases: first, the creation of a shared glossary, and second, the agreement on common definitions. The first phase has been **widely implemented** under Serbia's leadership as the adopter. In 2020, a dedicated website for the glossary was launched with the support of the Ministry of Interior of the Republic of Serbia and the University of Criminal Investigation and Police Studies.

[133] Kazakhstan's Representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Seventh Substantive Session (4-8 March 2024).

[134] Czech Republic as part of the OEWG Confidence Builders (2024): Joint Working Paper, How information sharing contributes to security and stability in cyberspace: Examples from Regional Points of contact networks.

[135] Germany as part of the OEWG Confidence Builders (2023): Input Paper, CBMs in Action.

The glossary currently includes over 2,000 terms and is supposed to be updated on a regular basis, at least once per year.[136]

The starting point for this initiative was the OSCE's POLIS platform, where, in 2020, a team of university students reviewed all 225 available documents and identified over 1,800 terms and definitions used by participating states, either in their national languages or in English. Implementation followed a structured process: defined terms were extracted from national legislation, along with their original-language definitions. In cases where states had officially published legal acts in English, both the term and its definition were included, where no official translation existed, only the term was translated, while the definition remained in the original language. The compiled list was then made available on the POLIS platform, and participating states were invited to review, comment, and provide missing English translations of definitions. This process resulted in the development of a glossary containing all terms defined by participating states. The initiative built on earlier work funded by Switzerland, notably a 2014 research study by the New America Foundation supporting implementation.[137]

Regarding the second step, it was decided that implementation is no longer an objective.[138] This position reflects broader international developments in cybersecurity, where it has become increasingly evident that agreeing on common definitions poses a major challenge, given that divergent political and ideological perspectives are often embedded in the terminology itself.[139] The OSCE's adoption of the term "cyber/ICT security" exemplifies this: it was a pragmatic compromise that enabled progress despite disagreements over terminology.

CBM 10

CBM 10 (2013): *"Participating States will voluntarily exchange views using OSCE platforms and mechanisms inter alia, the OSCE Communications Network, maintained by the OSCE Secretariat's Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs."*

[136] Nebojsa Jokic via OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[137] The results of this can be found here and here.

[138] The website notes: "[a]t this stage, we do not intend to undertake activities on producing a consensus glossary."

[139] Ghernaouti, Solange and Crespo, Laura (2017): Building Confidence in the Cyber Realm as a Means of Preventing Conflict - a Swiss Perspective. In: European Cyber Security Journal 3 (1), pp. 10-25. // Ben Hiller (2018): OSCE Experts: Cyber/ICT Security (Video Interview).

Background: This CBM encourages participating states to voluntarily exchange views and information through existing OSCE platforms, most notably the OSCE Communications Network maintained by the Conflict Prevention Centre. The goal is to facilitate secure communication on matters related to cyber/ICT confidence-building. Such exchanges can take the form of messages, alerts, or updates, aiming to foster cooperation and increase national cyber readiness.[140]

Practice: The OSCE Communications Network is a computer-based system linking participating states' capitals, maintained by the OSCE Secretariat's Conflict Prevention Centre. Its existence provides a strong foundation for implementing cyber CBMs within the OSCE, as it demonstrates that the organisation already has functioning infrastructure in place for secure communication, an area where the OSCE has long-standing experience and credibility.[141] In 2013, participating states agreed to explore the network's potential use for cyber/ICT security-related CBMs, and after extensive consultations, its application for this purpose was approved in 2017.[142] Today, the Communications Network facilitates the voluntary exchange of information – primarily threat reports – among an increasing number of connected states, reflecting that this CBM is **widely implemented**. It also serves as part of the OSCE's crisis communication mechanism in conjunction with CBM 3, CBM 8, and CBM 13.

CBM 11

CBM 11 (2013): *"Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include inter alia proposals from the Consolidated List circulated by the Chairmanship of the IWG under PC.DEL/12/682 on 9 July 2012, subject to discussion and consensus agreement prior to adoption."*

Background: This CBM establishes a regular dialogue mechanism requiring participating states to meet at least three times per year through the IWG under

[140] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[141] Teddy Nemeroff via OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[142] OSCE (2017): Decision No. 5/17. Use of the OSCE Communications Network to Support Implementation of Permanent Council Decisions No. 1039, No. 1106 and No. 1202.

the Security Committee.[143] Here, national delegations, consisting of cyber diplomats and cybersecurity policy experts, meet to review the implementation of existing cyber CBMs, share national updates, and consider the development of new measures based on previously proposed ideas, such as those from the 2012 Consolidated List. Operating by consensus, the IWG promotes cooperation by facilitating the exchange of knowledge, experiences, and best practices among participating states.[144]

Practice: This CBM has been **widely implemented** for years: participating states, represented by their designated national experts, convene in the IWG up to four times per year, which is more than the three meetings initially aimed for. These meetings provide a central platform for exchanging views on cyber/ICT security issues and advancing the practical implementation of CBMs. The IWG is chaired by a designated leader who sets the agenda, with a standing item for sharing national implementation updates,[145] which are delivered through a tour de table, often complemented by presentations on national cybersecurity strategies, PPPs, and specific CBM activities presented by the corresponding adopters. The OSCE Secretariat's TNTD also provides updates, such as the results of CommsChecks under CBM 8. Meetings are frequently held alongside implementation activities, including tabletop exercises and conferences like the annual CiO conference in the chairing state, offering opportunities for in-person engagement and helping to put a face on PoC contacts, thereby strengthening the human network supporting CBM implementation.

This CBM is cross-cutting, linked to many other CBMs focused on information exchange and monitoring the broader framework. Its implementation is verifiable, with regular meetings and consistently high participation over the years.[146] Regarding the possibility of adopting further CBMs, as mentioned in CBM 11, it is worth noting that five additional CBMs were adopted in 2016 (CBM 12-16). However, in 2017, it was decided not to adopt any more cyber CBMs at this time, and to focus on implementing the existing ones instead.[147]

[143] Established under OSCE (2012): Permanent Council Decision No. 1039. Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.

[144] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[145] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[146] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[147] OSCE (2017): Ministerial Council Decision No 5/17. Enhancing OSCE Efforts to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.

CBM 12

CBM 12 (2016): *"Participating States will, on a voluntary basis, share information and facilitate inter-State exchanges in different formats, including workshops, seminars, and roundtables, including on the regional and/or subregional level; this is to investigate the spectrum of co-operative measures as well as other processes and mechanisms that could enable participating States to reduce the risk of conflict stemming from the use of ICTs. Such activities should be aimed at preventing conflicts stemming from the use of ICTs and at maintaining peaceful use of ICTs. With respect to such activities participating States are encouraged, inter alia, to:*

> - *Conduct such activities in the spirit of enhancing inter-State co-operation, transparency, predictability and stability;*
> - *Complement, through such activities, UN efforts and avoid duplicating work done by other fora; and*
> - *Take into account the needs and requirements of participating States taking part in such activities.*

Participating States are encouraged to invite and engage representatives of the private sector, academia, centres of excellence and civil society in such activities."

Background: This CBM encourages participating states to voluntarily share information on regional and sub-regional activities and to organise or engage in cooperative initiatives at the national, regional, or subregional level. Its objective is to enhance transparency through the exchange of experiences and best practices while aligning with and complementing UN processes. Activities under this CBM are often inclusive, involving stakeholders such as the private sector, academia, and civil society, highlighting the importance of a multi-stakeholder approach to cybersecurity. Overall, CBM 12 aims to foster cooperation by supporting joint confidence-building efforts and promoting the sharing of knowledge and best practices.[148]

Practice: To implement this CBM, participating states voluntarily share information and engage in inter-state exchanges through workshops, seminars, and roundtables at the national, regional, and subregional levels.[149] Since 2017, the OSCE has organised subregional trainings bringing together small groups of states

[148] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[149] EU's Representative (2025): (5th meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025).

to share national updates and participate in tailored cybersecurity exercises.[150] Many of these activities also support the implementation of other CBMs, such as workshops under CBM 6 (as part of the “regional capacity-building project on combating cybercrime in Central Asia”) or CBM 2 and CBM 4, making this CBM inherently cross-cutting and often implemented implicitly. CBM 12 is especially resource intensive, and is adopted by the EU, Switzerland, North Macedonia, and Poland.[151]

The OSCE Secretariat’s TNTD also engages in cross-regional exchange, for example, through participation in the UN OEWG as well as the 2024 ECOWAS study visit to the OSCE, organised by the EU, Germany, and the CBM adopters, which aimed to share best practices on developing and operationalising CBMs and discuss potential implementation challenges. Representatives from the AU and the OAS also attended, further strengthening cross-regional dialogue.[152] Overall, this CBM is **implemented, but not widely** yet.

CBM 13

CBM 13 (2016): *“Participating States will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests. This does not exclude the use of the channels of communication mentioned in Permanent Council Decision No. 1106.”*

Background: This CBM encourages participating states to voluntarily organise activities to improve the understanding and use of secure and authorised communication channels for managing ICT-related incidents. The goal is to prevent misperceptions or unintended escalation by clarifying how to respond to technical, legal, or diplomatic requests, particularly during times of heightened cyber tension. These efforts complement existing OSCE communication mechanisms, such as those established under the first set of CBMs. This CBM is connected to CBMs 3, 8, and 10 as part of the crisis communication mechanism.

[150] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[151] EU’s Representative (2025): (5th meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025).

[152] EU as part of a group at the OEWG (2025): Non-Paper. Inter-regional Cooperation - The Role of Regional Organizations in Implementing the UN Framework for Responsible State Behaviour in Cyberspace.

Practice: Adopted by the United States, this CBM has been **widely implemented** through two main approaches: first, participating states leveraged the existing OSCE Communications Network as a secure and confidential channel for sharing notifications about ICT-related incidents with potential national security implications (CBM 10), thereby avoiding the need to create new infrastructure. Today, most states are connected to the network, with participation steadily increasing. Second, states established nine standardised templates to structure communications – covering incident reporting, information requests, expressing concerns, or seeking consultations – enhancing clarity, consistency, and coordination.[153] Tabletop exercises conducted under CBM 3 further support CBM 13 by allowing states to practice using the secure channels and reinforcing their operational readiness.

CBM 14

CBM 14 (2016): *"Participating States will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs."*

Background: This CBM recognises that most critical ICT infrastructure is owned and operated by private actors, making PPPs essential for addressing shared cybersecurity threats.[154] It encourages participating states to voluntarily foster collaboration between governments and the private sector and to establish mechanisms for exchanging best practices in incident response, threat mitigation, and resilience-building. Thus, the CBM describes steps to consider at the national level.[155]

Practice: In 2021, the states that adopted CBM 14 – Austria, Belgium, Estonia, Finland, Italy, and Sweden (later joined by Bosnia and Herzegovina) – initiated a study titled "Report on Main Insights from the OSCE Cyber/ICT Security Confidence-Building Measure 14 Questionnaire on Public-Private Partnerships." Based on a questionnaire sent to all participating states, it assessed engagement with CBM 14 and mapped emerging practices in cybersecurity-related PPPs.

[153] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[154] Gertz, Geoffrey, and Evers, Miles (2020): Geoeconomic Competition: Will State Capitalism Win? In: Washington Quarterly 43 (2), pp. 117–136.

[155] Minárik, Tomáš (2016): OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection.

Building on this effort, the OSCE Secretariat's TNTD, together with two researchers, published a good practice report in 2023 showcasing real-world examples and offering baseline recommendations to support future PPP initiatives.[156] The findings demonstrate that significant attention has been to the objective of CBM 14, with numerous states – including the UK, Albania, Czech Republic, Denmark, Estonia, Finland, Italy, Slovakia, Serbia, Türkiye, the US, and the EU – recognising PPPs in national policy frameworks, legislation, or cybersecurity strategies. For example, the UK's 2022 National Cyber Security Strategy emphasises a whole-of-society approach with enduring partnerships across the public, private, and third sectors.

The implementation of CBM 14 is further supported through the IWG. In rare cases, these meetings also include external stakeholders, such as private sector representatives and academic experts who contribute input and share experiences.[157] As the report highlights, "some participating States have noted that lessons shared on CBM 14 implementation within the (...) [IWG have] been very useful, helping them shape similar initiatives in their own countries, redesign or redirect them." It further notes that "[t]here is a clear appetite among most participating States to continue sharing emerging practices and lessons on cybersecurity-related public-private partnerships within the OSCE framework."[158]

CBM 14 functions primarily as a strategic objective rather than a narrowly defined measure. Many of its envisioned initiatives, such as enhancing national cyber resilience through collaboration with private actors, occur implicitly, thereby fulfilling its goals. Information exchange on national approaches and best practices is therefore central in analysing its implementation. Moreover, OSCE capacity-building activities frequently involve various non-state actors, implicitly advancing CBM 14 by fostering inclusive dialogue and multi-stakeholder cooperation. Overall, this CBM is **widely implemented**, however, a lot of it happens implicitly.

CBM 15

CBM 15 (2016): *"Participating States, on a voluntary basis, will encourage, facilitate and/or participate in regional and subregional collaboration between*

[156] You can find the report, titled "Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States", which includes a great collection of examples for such ppp-initiatives within the OSCE participating states, here.

[157] Sziliva Tóth in 2023 on the "Inside Cyber Diplomacy"-Podcast by James Lewis and Christopher Painter in the episode "Implementing Cyber Confidence-Building Measures".

[158] OSCE (2023): Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States.

legally authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies. Collaboration may, inter alia, include:

> - *Sharing information on ICT threats;*
> - *Exchanging best practices;*
> - *Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure;*
> - *Adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident;*
> - *Sharing national views of categories of ICT-enabled infrastructure States consider critical;*
> - *Improving the security of national and transnational ICT-enabled critical infrastructure including their integrity at the regional and subregional levels; and*
> - *Raising awareness about the importance of protecting industrial control systems and about issues related to their ICT-related security, and the necessity of developing processes and mechanisms to respond to those issues."*

Background: This CBM encourages participating states to voluntarily collaborate at the regional and subregional levels – for example, via CERTs and critical-infrastructure regulators – to strengthen the security and resilience of ICT-dependent critical infrastructure, while also considering steps at the national level. Suggested activities include sharing threat intelligence, exchanging best practices, coordinating crisis management plans for cross-border incidents, harmonising incident classification schemes, and raising awareness on the protection of industrial control systems. This CBM underscores the importance of a comprehensive, multi-stakeholder approach by actively involving diverse actors, while standing out from other CBMs for its more technical focus.

Practice: Progress has been made in the implementation of this CBM in recent years. Many activities under CBM 15 are closely connected to others, for example, CBM 1 on sharing ICT threat information, CBM 9 on mapping critical infrastructure definitions, and CBM 3 on crisis communication and management. Workshops organised within the OSCE framework also indirectly contribute to its implementation.

A central focus of implementation has been the development of voluntary national arrangements for classifying ICT incidents by scale and seriousness, commonly known as national cyber incident severity scales (NCISS). Such systems are vital for prioritising responses to incidents affecting critical infrastructure and for strengthening both national and international crisis communication by fostering transparency, predictability, and a shared understanding of incident severity. They also help states to "speak the same language" when responding to cyber threats, thereby reducing the risk of misunderstandings.[159]

To support this, the OSCE Secretariat's TNTD has implemented, since 2021, the "Facilitation of the development and implementation of national cyber incident severity scales (NCISS) and related measures to protect critical infrastructures" project, focused on CBMs 15 and 3 and funded by France and Germany.[160] Within this framework, customised support has been provided to Uzbekistan, Moldova, and Ukraine.[161] These activities have explored the rationale for establishing severity scales, supported their development and implementation, and enabled the exchange of best practices, including through practical simulations involving hypothetical cyber operations on critical infrastructure, workshops, and best practice exchanges.[162]

Parallel efforts have reinforced this work: in 2020, France launched a survey to identify participating states' needs regarding severity scales,[163] followed in 2022 by a TNTD study analysing emerging practices. That same year, a good practice report on cyber incident classification was published, highlighting common approaches, challenges, and lessons learned. Despite some differences, the report concluded that the lessons learned serve as a valuable capacity- and trust-building tool to promote the broader use of such systems within the OSCE region and beyond. The adopters of this CBM circulated a new survey in 2024 to update the overview of national measures. In 2025, another handbook on national cyber incident classification was published, drawing on survey results and offering a step-by-step guide for developing and implementing NCISS. The handbook aims to support participating states in increasing this CBM's implementation rate.

Today, many participating states have either established or are developing classification systems (35 out of 57 participating states),[164] often backed by

[159] OSCE (2022): Cyber Incident Classification. A Report on Emerging Practices within the OSCE region.

[160] Find more on it here.

[161] OSCE's Representative (2025): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025).

[162] Find an example of such a workshop in Vienna in 2024 here, or in Moldova in 2024 here, or in Bosnia-Herzegovina in 2022 here, or in Ukraine in 2025 here, as well as in Uzbekistan in 2023 and 2024.

[163] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[164] OSCE (2025): National Cyber Incident Classification.

new legal or policy frameworks. Within the EU, the NIS Directive has ensured that such systems exist in (almost) all EU member states[165] (although developed independently of this CBM, they still contribute to its objectives). Other states, including the USA and UK also maintain similar frameworks.[166] Overall, the CBM is **widely implemented**, however, a lot of it happens implicitly.

CBM 16

CBM 16 (2016): *"Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing co-operation and transparency within the OSCE region. OSCE participating States agree that such information exchange, when occurring between States, should use appropriately authorized and protected communication channels, including the contact points designated in line with CBM 8 of Permanent Council Decision No. 1106, with a view to avoiding duplication."*

Background: This CBM encourages participating states to promote responsible vulnerability disclosure and to share information on remedies, particularly with private actors. This includes fostering CVD policies and establishing national processes.[167] It emphasises the need for a multi-stakeholder approach, thereby linking it closely to CBM 14 on PPPs. To safeguard sensitive information exchanges, it also points to the possible use of CBM 8's secure communications framework. Overall, it seeks to foster cooperation and transparency among states and stakeholders.[168]

Practice: The Netherlands, Czech Republic, Hungary, and Romania have assumed responsibility as adopters of this CBM. One concrete measure has been the development of a publicly available e-learning course on CVD by the OSCE Secretariat's TNTD. This course introduces CVD as a tool to strengthen cyber

[165] NIS Cooperation Group (2018): Cybersecurity Incident Taxonomy. CG Publication 04/2018.

[166] OSCE (2022): Cyber Incident Classification. A Report on Emerging Practices within the OSCE region.

[167] The international standard ISO/IEC 29147:2018 defines vulnerability disclosure as a cooperative process between vendors and security researchers to report, coordinate, and publish information about vulnerabilities and their resolution. Coordinated Vulnerability Disclosure (CVD) ensures vulnerabilities are addressed in a timely manner, risks are minimized, and users receive sufficient information to protect their systems. At the national level, CVD policies provide structured frameworks for responsible reporting, vendor response, and researcher protection - strengthening cybersecurity and promoting awareness of emerging threats.

[168] Carmen Gonsalves (2022) via OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

resilience, covering key actors, process steps, and legal challenges, and concludes with a fictional scenario to illustrate practical application. Within this framework, the Netherlands shares information on its national CVD guidelines,[169] which assist companies and organisations in setting up their own policies. While such initiatives contribute to CBM implementation, they are also pursued independently of the OSCE framework, thus implicitly fulfilling the CBM's objectives.

Workshops have also been organised to advance CBM 16, such as a 2023 event in Istanbul, where good practices and examples of national implementation were presented, and participants engaged in a practical exercise to better understand the nuances of vulnerability disclosure.[170] These activities highlight growing engagement but also show that implementation remains limited in scope. Overall, only a small number of states have national CVD policies in place.[171] This CBM can therefore be considered **implemented, but not widely**.

4.1.3. Adopt-a-CBM-initiative as implementation driver

The OSCE has long-standing experience with CBMs, dating back to the Cold War, and was the first multilateral organisation to adopt CBMs specifically for the cyber domain. Since then, notable progress has been achieved, and the OSCE has established itself as a key multilateral forum contributing to the promotion of security and stability in the cyber domain.[172] The OSCE cyber/ICT security CBMs address a range of issues and are grouped into three functional categories:[173]

- **Posturing CBMs** (CBMs 1, 4, 7, 9, 10) are intended to make state behaviour in cyberspace more transparent and predictable, allowing states to read each other's postures.
- **Communication CBMs** (CBMs 3, 5, 8, 11, 13) promote timely dialogue and cooperation to prevent misunderstandings and defuse tensions.
- **Preparedness CBMs** (CBMs 2, 6, 12, 14, 15) support national readiness and due diligence to address cyber threats, by further developing national capacities.

[169] You can find the Dutch guidelines on CVD here.

[170] See here.

[171] ENISA (2022): Coordinated Vulnerability Disclosure Policies in the EU. // Herpig, Sven (2024): Vulnerability Disclosure: Guiding Governments from Norm to Action.

[172] Ghernaouti, Solange and Crespo, Laura (2017): Building Confidence in the Cyber Realm as a Means of Preventing Conflict - a Swiss Perspective. In: European Cyber Security Journal 3 (1), pp. 10-25.

[173] Radicevic, Velimir (2018): The Role of OSCE Confidence-Building Measures in addressing cyber/ICT security challenges. // Greminger, Thomas (2019): Opening Remarks, Vienna Cyber Security Week 2019.

Implementation has been advanced through a wide array of activities, including workshops, tabletop exercises, e-learning modules, reports, and by the establishment of regular meetings, communication formats, and information exchange mechanisms. Many of these activities are carried out under the "Activities and Customized Support for the Implementation of OSCE Cyber/ICT Security Confidence-Building Measures" project, supported by voluntary financial contributions from participating states. Others are funded through dedicated projects tied to individual cyber CBMs, such as CBMs 3, 15, and 8. Given the diverse levels of cyber maturity across the OSCE region, these initiatives often serve a dual purpose of both implementation and capacity-building.

A key driver of implementation has been the Adopt-a-CBM-initiative launched in 2018. Under this framework, participating states assume ownership of specific CBMs by developing discussion papers outlining implementation pathways, conducting questionnaires to map national approaches, and organising supporting activities.[174] However, not all cyber CBMs have been adopted, adoption status can change over time, and not all adopters are made public. While transparency on adoption could further strengthen ownership, as of the time of writing, 26 adopters have been identified across 11 of the 16 cyber CBMs.

The OSCE Secretariat's TNTD also plays a central role in supporting implementation. It assists participating states by raising awareness, building capacity, and conducting implementation-related activities.[175] It manages the CBM 8 PoC network, and facilitates ComsChecks, PoC meetings, and the IWG under CBM 11. These CBMs form the backbone of the OSCE's cyber CBM architecture and can be considered cornerstones of the confidence-building framework in the cyber domain.While the systematic verification of implementation has not been undertaken, it is clear that 98% of participating states have implemented at least one cyber CBM nationally (most probably at least CBM 8 by designating a national PoC) and are actively engaging in related processes.[176] However, priorities differ across states, reflecting varying political interests and capacities.[177]

While some of the cyber CBMs include clearly verifiable deliverables, such as nominating national PoCs (CBM 8), sharing national strategies (CBM 7),

[174] OSCE (2023): 10 Years of OSCE/ICT Security Confidence-Building Measures.

[175] Toth, Szilvia (2025): Regional Organisations and Confidence-Building Measures. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James (Eds.): A Handbook for the Practice of Cyber Diplomacy. EU Institute for Security Studies.

[176] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[177] Radicevis, Velimir (2017): Promoting Cyber Stability between States: OSCE Efforts to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies (ICTs) in the Context of Global and Regional Security. In: IFSH: OSCE Yearbook.

establishing a glossary of definitions (CBM 9), or participating in the IWG (CBM 11), others require states to take action at the national level, such as establishing legal frameworks for cooperation on cybercrime (CBM 6), developing PPPs (CBM 14), or implementing a national cyber incident severity scale (CBM 15). Finally, some cyber CBMs are more broadly worded and can be interpreted as commitments to particular objectives, with implementation left open to a range of possible actions. For instance, CBM 4 and 5 can involve a variety of activities not always explicitly labelled as CBM implementation but which nevertheless contribute to their goals. Often, these measures align with national priorities to enhance cybersecurity and resilience regardless of their link to cyber CBMs. In such cases, the confidence-building effect derives more from the exchange of experiences and best practices.

The interconnected nature of CBMs is also notable:[178]

- CBMs 2, 4, and 6 promote cyber resilience and preparedness and are often supported through joint workshops.
- CBMs 3, 8, 10, and 13 encourage communication, representing a mechanism for crisis response.
- CBMs 1, 7, and 9 enhance transparency.
- CBMs 5, 10, 11, and 12 focus on practical cooperation.
- CBMs 14, 15, and 16 aim to strengthen multi-stakeholder engagement.

However, the cyber domain does not exist in isolation. As noted, “Europe is experiencing its most severe security crisis in many decades.”[179] Russia’s war of aggression against Ukraine has fundamentally eroded trust: “Trust takes years to build, but only seconds to break, and Russia’s military aggression against Ukraine, including its use of malicious cyber operations, is therefore not only illegal and unjustifiable – it also constitutes a breach of international commitments and runs directly counter to confidence-building efforts.”[180]

Despite this severe geopolitical crisis, cyber and ICT security remain areas where cooperation continues to some extent. Implementation activities persist,[181] and some states have even deepened engagement. For instance, Germany reported

[178] OSCE (2021): OSCE Cyber/ICT security Confidence-Building Measures. E-Learning Course.

[179] Germany’s representative (2023): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Fourth Substantive Session (6-10 March 2023).

[180] Denmark’s representative (2022): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Second Substantive Session (9-13 March 2022).

[181] Toth, Szilvia (2025). Regional Organisations and Confidence-Building Measures. In: A Handbook for the Practice of Cyber Diplomacy.

that it began sharing information on major cyber incidents more actively through the OSCE PoC Network from May 2022 onward, specifically in response to "heightened geopolitical tensions in the OSCE area."[182] In this sense, the crisis has brought some states closer together. Yet at the same time, it has pushed the organisation as a whole into a difficult position, as other areas of cooperation remain blocked[183] and the task of rebuilding lost trust is proving to be a complex and lengthy process.

4.2. Organization of American States (OAS)

4.2.1. Formulation of OAS cyber CBMs

The Organization of American States (OAS), founded in 1948, is a regional body comprising 35 states[184] across the Americas, as well as the Caribbean. Its core mission is to promote democracy, human rights, security, and development through political dialogue, cooperation, and legal frameworks.[185]

The OAS has, in recent years, increasingly focused on cybersecurity as a key aspect of regional stability. Its primary contribution has been capacity-building efforts led by the Inter-American Committee Against Terrorism (CICTE), the OAS main body for cybersecurity implementation, which supports its members in developing national cybersecurity strategies, strengthening incident response capabilities, and providing political and technical assistance through programmes aimed at preventing and countering cyber threats.[186] In April 2017, a resolution[187] proposed by Chile, Colombia, Peru, Costa Rica, Canada, Guatemala, and Mexico[188] establishing a working group on Cyber CBMs[189] as a subsidiary body to the CICTE was adopted, focusing on what the OAS refers to as non-traditional CBMs.

[182] Germany as part of the OEWG Confidence Builders (2023): Input Paper, CBMs in Action.

[183] Hernández, Gabriela (2023): OSCE in Crisis Over Russian War on Ukraine.

[184] Antigua and Barbuda, Argentina, Bahamas, Barbados, Belize, Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Cuba (currently does not participate in OAS activities), Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haití, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, Trinidad and Tobago, United States, Uruguay, and Venezuela.

[185] Find more information here.

[186] Find more here.

[187] OAS CICTE (2017): CICTE/RES.1/17. Establishment of a Working Group on Cooperation and Confidence-Building Measures in Cyberspace.

[188] Francisco Ferrada, Mila, and Castro Hermosilla, Pablo (2019): The current process of OAS confidence-building measures in cyberspace. In: GFCE Magazine (6), pp. 17-20.

[189] See here.

The working group aims “to strengthen cooperation, transparency, predictability and stability among OAS States in the use of cyberspace and to help support implementation of UN relevant decisions (...) at the regional level.”[190] Since then, OAS member states have agreed on 11 cyber CBMs.[191]

4.2.2. Implementation of OAS cyber CBMs

CBM 1

CBM 1 (2018): *“Provide information on national cybersecurity policies, such as national strategies, white papers, legal frameworks and other documents that each Member State considers relevant.”*

Background: CBM 1 is designed to foster transparency and predictability among OAS member states in the field of cybersecurity by openly sharing strategic objectives, priorities, and governance structures related to national cybersecurity. This measure enables partners to anticipate each other’s actions and policies in the cyber domain, thereby reducing the risk of misperceptions.

Practice: When this CBM was adopted in 2018, many OAS member states were still in the early stages of developing their national cybersecurity policies. Since then, progress has been steady: member states now regularly report on their developments, experiences, and challenges during the annual meetings of the CBM Working Group, in line with the CBM’s transparency goals. Recognising the varying levels of capacity across the region, the CICTE Secretariat has taken a proactive role in supporting member states, for example by providing direct support to Mexico and Ecuador in formulating their national cybersecurity strategies. These targeted efforts have helped ensure that more states are now in a position not only to develop but also to share their cybersecurity policies.[192]

To streamline implementation, the CICTE Secretariat developed a standardised template with key fields, such as policy title, description, responsible institutions, effective date, and reference link.[193] Member states are invited to voluntarily

[190] OAS as part of an open, informal, cross-regional group (2025): Non-Paper on Inter-regional Cooperation. The Role of Regional Organizations in Implementing the UN Framework for Responsible State Behaviour in Cyberspace.

[191] Find them here.

[192] A further resource supporting this progress is the 2022 publication titled “National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and other Regions.”

[193] OAS CICTE (2021): Report on Cooperation and Confidence-Building Measures in Cyberspace. OAS/Ser.L/X.5. CICTE/GT/MFCC-22/21.

complete and submit this template, contributing to a centralised repository of national cybersecurity documentation. Since 2021, CBM 1 has also been supported by a secure web portal accessible to designated PoCs (see CBMs 2 and 3) from each member state. Maintained by the CICTE Secretariat[194] and regularly updated to improve usability, the portal facilitates the exchange and retrieval of national cybersecurity policies.[195] The number of states sharing documents through the portal has steadily increased, and today approximately 70% of OAS member states actively share their policies, either via the web portal or directly during CBM Working Group meetings. Therefore, this CBM is **widely implemented**. The Secretariat continues to encourage and support states in formulating such documents, creating clear synergies between the capacity-building dimension of CBMs 1 and 4.

CBM 2

CBM 2 (2018): *"Identify a national point of contact at the political level to discuss the implications of hemispheric cyber threats."*

Background: CBM 2 aims to enhance regional cyber stability by designating national PoCs at the political level that provide a reliable channel for timely, high-level communication between states in response to cyber incidents, helping to clarify intent, share information, and prevent escalation. In this context, member states emphasise the importance of recognising that ICT-related incidents often originate from, or impact, third countries. Thus, when a state is contacted regarding such an incident, this should not be interpreted as an accusation of involvement or wrongdoing. Instead, communication via the PoCs established under CBM 2 is intended to facilitate dialogue and clarification. At the same time, the initiation of contact indicates that the reporting state considers the incident potentially relevant to its national security.[196] Overall, the measure strengthens trust and cooperation by ensuring that every member state has a known and dependable channel for diplomatic engagement in cybersecurity matters.[197]

[194] OAS CICTE (2019): Second Meeting of the Working Group on Cooperation and Confidence Building Measures in Cyberspace. Rapporteur Report. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.16/19.

[195] OAS CICTE (2024): Report of the Fifth Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.14/24.

[196] OAS CICTE (2019): Draft Regional Confidence-Building Measures (CBMs) to Promote Cooperation and Trust in Cyberspace. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.12/19 rev. 2.

[197] OAS CICTE (2019): Second Meeting of the Working Group on Cooperation and Confidence Building Measures in Cyberspace. Rapporteur Report. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.16/19.

Practice: CBM 2, though adopted earlier, has been implemented in parallel with CBM 3, which focuses on contacts within Ministries of Foreign Affairs (MFAs). While both measures involve the nomination of national PoCs, CBM 2 PoCs operate at the strategic and political levels, complementing the work of law enforcement, CSIRTs, and other technical actors engaged in combating cybercrime and managing technical incidents.[198]

Each member state is responsible for designating a policy-level PoC and keeping that information regularly updated.[199] These individuals should be strategically positioned within government and supported by institutional structures that enable meaningful engagement in cybersecurity matters. To complete a PoC profile, the following details are shared: country, full name, official position, affiliated institution, email address, and category of designation (cyber policy or foreign affairs contact). The CICTE Secretariat maintains the official PoC Directory and ensures secure access for authorised users via the web portal, which since its launch in 2021 has served as the primary tool for maintaining and sharing PoC information, accessible only to nominated contacts.[200]

A clearly defined procedure governs the use of the PoC system during cyber incidents, requiring timely responses in a spirit of cooperation and shared interest in preventing escalation.[201] A notable example occurred in 2022 during a major

[198] Defined here.

[199] OAS CICTE (2021): Report on Cooperation and Confidence-Building Measures in Cyberspace. OAS/Ser.L/X.5. CICTE/GT/MFCC-22/21.

[200] OAS' Representative (2022): (7th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Third Substantive Session (25-29 July 2022).

[201] OAS CICTE (2019): Draft Regional Confidence-Building Measures (CBMs) to Promote Cooperation and Trust in Cyberspace. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.12/19 rev. 2.

"Procedure for making an inquiry:

1. Refer to the contact list to find the appropriate POC from the participating Member States from whose territory the cyber activity is emanating.
2. Call or email the relevant POC and provide your name and affiliation.
3. Inform the POC that you are invoking OAS CBM #2 in accordance with paragraph 78 of the OAS General Assembly Resolution AG/RES. 2925 (XLVIII-O/18), and that you are contacting the person in question because they are listed as their participating Member State's POC.
4. Describe the nature of the incident.
5. Ask for additional information about the incident and provide your contact information. Indicate time sensitivity as appropriate.

Procedure for responding to an inquiry:

6. Option 1: Provide an immediate response to the cyber incident query (if possible).
7. Option 2: Inform the POC that you will look into the cyber incident and, follow up with additional information, as possible. Ask for the POC's contact information. Provide an estimated timeframe for a response, as appropriate.

CBM POCs should engage cyber counterparts within their own government or private sector as necessary to collect information and develop an appropriate response. Governments should also consider standing up a consultative working group, if none exist, to ensure officials know whom to contact in order to generate responses in a timely manner."

ransomware campaign by the Conti group,[202] which "marked a turning point for regional cybersecurity collaboration" by underscoring the necessity of timely information sharing.[203]

To further operationalise the CBM, the CICTE Secretariat has organised targeted activities, including a workshop on the role of PoCs and a scenario-based tabletop exercise during the second Working Group Meeting in 2019, which tested the effectiveness of the PoC network under simulated crisis conditions. CBM 2 PoCs also benefit from access to CICTE's training and capacity-building programmes, as well as the dedicated web portal – efforts designed to foster community, trust, and shared purpose. Implementation is additionally reinforced by synergies with CBMs 4, 5, and 6. To ensure readiness, the Secretariat conducts regular ping tests of the PoC network, reporting consistently high response rates.[204] Looking forward, it plans to continue these tests and expand tabletop exercises to further strengthen communication and responsiveness.

Participation in the PoC Directory has risen steadily, and by 2025, it included 84 Cyber Policy Points of Contact, 22 of whom represent MFAs (CBM 3).[205] This reflects near-universal engagement by member states and underscores CBM 2's foundational role within the broader CBM framework. Indeed, CBMs 2 and 3 remain the most **widely implemented**, serving as cornerstones of the regional architecture for cyber stability. Building on this solid base, efforts are now underway to align the OAS PoC Directory with the UN PoC Directory to improve cross-regional coordination, a proposal discussed among member states on the margins of the 2025 OEWG meeting, where it received broad support.[206]

CBM 3

CBM 3 (2019): *"Designate points of contact, if they do not currently exist, in the Ministries of Foreign Affairs with the purpose of facilitating work for cooperation and international dialogues on cybersecurity and cyberspace."*

[202] Murray, Christine, and Srivastava, Mehul (2022): How Conti ransomware group crippled Costa Rica - then fell apart.

[203] Argentina, Brazil, Chile, Colombia, Dominican Republic, Mexico and Uruguay as part of the OEWG Confidence Builders (2024): Joint Working Paper. How information sharing contributes to security and stability in cyberspace: Examples from Regional Points of contact networks.

[204] Colombia as part of the OEWG Confidence Builders (2023): Input Paper, CBMs in Action.

[205] See here.

[206] OAS CICTE (2024): Concept Paper. Consideration of How to Leverage the Existing OAS POC Directory with Respect to the newly established UN OEWG cyber POC Network. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.12/24. // OAS CICTE (2024): Report of the Fifth Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.14/24.

Background: CBM 3 calls on OAS member states to designate PoCs within their MFAs to strengthen international cooperation on cybersecurity and cyberspace issues. Adopted one year after CBM 2, this measure responded to a clear regional need: integrating MFAs more directly into cybersecurity governance. Traditionally, cybersecurity was viewed primarily as a technical issue, with MFA involvement often seen as secondary or even unnecessary. Yet diplomatic-level contacts play a vital role in facilitating dialogue, coordinating regionally and internationally, and aligning cybersecurity with broader foreign policy priorities.[207] By formalising MFA involvement, CBM 3 underscores that cybersecurity is not only a technical challenge but also a strategic foreign policy priority, one that must be embedded within each state's national cybersecurity architecture.[208] In doing so, it establishes formal channels for cyber diplomacy, strengthening the region's ability to engage in multilateral discussions, respond collectively to cyber incidents, and promote responsible state behaviour in cyberspace.

Practice: The implementation of CBM 3 builds directly on the foundation established by CBM 2, with both measures working in tandem to strengthen communication and coordination at the political and diplomatic levels. As with CBM 2, a complete PoC profile must include key details such as the individual's name, position, institution, and contact information. This information is maintained in the secure web portal managed by the CICTE Secretariat, which facilitates access for authorised users and ensures regular updates.[209] Requests for information and the exchange of data through the directory follow the same procedures as outlined for CBM 2. MFA PoCs are also encouraged to take part in cyber-related capacity-building initiatives and diplomacy-focused trainings under CICTE's capacity-building framework framework,[210] creating natural synergies with CBMs 4, 5, and 6.

As of 2025, 22 MFA PoCs have been formally nominated and registered in the web portal, reflecting that the CBM is **widely implemented**.[211] These contacts frequently serve as the primary actors in regional and international cyber diplomacy. Efforts are also underway to align the OAS PoC Directory with the UN's cyber diplomacy

[207] OAS CICTE (2019): Second Meeting of the Working Group on Cooperation and Confidence Building Measures in Cyberspace. Rapporteur Report. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.16/19.

[208] OAS CICTE (2019): Second Meeting of the Working Group on Cooperation and Confidence Building Measures in Cyberspace. Rapporteur Report.

[209] See here.

[210] OAS' Representative (2022): (7th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Third Substantive Session (25-29 July 2022).

[211] See here.

contact list, further reinforcing CBM 3's role in bridging regional and global cybersecurity cooperation.

Together with CBM 2, this measure has already had a tangible impact by providing the foundation for deeper cooperation. As Chile noted, "The PoCs have contributed to the exchange of information, strengthening cooperation on capacity-building and technical assistance, coordinating policies and positions with other states on multilateral and regional processes, responding to queries and requirements from other states and international stakeholders, requesting information on cyber-attacks and strengthening bilateral relations, among others."[212]

CBM 4

CBM 4 (2019): *"Develop and strengthen capacity building through activities such as seminars, conferences, and workshops, for public and private officials in cyber diplomacy, among others."*

Background: The effective implementation of cyber norms and agreements depends not only on political will but also on states' ability to understand, interpret, and operationalise them, underscoring the central importance of capacity development not only for public sector but also for private sector officials. Regional organisations like the OAS play a vital role in this process by ensuring that no state is left behind and by helping build strong national capabilities. CBM 4 thus exemplifies the OAS' strong emphasis on capacity-building and reflects a region-specific need to expand and deepen cyber-related expertise through targeted activities.[213]

Practice: This CBM is supported by the Cyber Diplomacy Training Program, planned and coordinated by the CICTE Secretariat, which plays a central role in its implementation.[214] Over the past few years, numerous courses have been organised for officials working on cybersecurity within member states. The trainings vary in thematic focus and are tailored to different CBM-related topics. In recent years, workshops and masterclasses have covered CBMs in general, international cyber diplomacy, international law and norms in cyberspace, state responses to cyber

[212] Chile as part of the OEWG Confidence Builders (2023): Input Paper, CBMs in Action.

[213] Barret, Kerry-Ann (2025): Cybersecurity and Its Influence on Traditional Diplomacy in the Americas. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James (Eds.): A Handbook for the Practice of Cyber Diplomacy. EU Institute for Security Studies.

[214] OAS CICTE (2024): Presentation. Working Group on Cooperation and Confidence-Building Measures in Cyberspace.

operations, cyber diplomacy and critical infrastructure, gender and cybersecurity, digital rights and freedoms, IHL in cyberspace, the Programme of Action (PoA), the PoC Directory, and critical cybersecurity infrastructure, among others. The CICTE Secretariat aims to host one such workshop approximately every three months.[215] Acknowledging the diverse needs and capacities of its member states, the OAS adapts its training programmes to address country-specific challenges. This tailored approach ensures that all states – regardless of cyber maturity – can meaningfully engage in and benefit from the implementation of cyber CBMs.[216]

For the masterclasses, states nominate participants, with professional profiles prioritized depending on the topic. In particular, the designated PoCs are up first for participation, making these trainings a key space for fostering trust and communication. This highlights the synergies between CBMs 2, 3, and 4, as the courses deepen relationships and practical cooperation among PoCs. Since 2017, the OAS has trained over 850 officials through more than 30 courses, reaching participants from over 30 member states.[217] Some of these courses are explicitly connected to CBM 4, while others contribute implicitly, reflecting the CBM's broad scope. It can thus be observed that the CBM is **widely implemented**. The development of these efforts can be roughly traced across three phases: pre-COVID, the focus was on general introductory training to address differing levels of cyber maturity; during COVID, webseminars were also delivered, however, there was a lack of in-person meetings; and post-COVID, more specialised masterclasses were introduced and delivered both online and in person. One idea is to consolidate knowledge through the development of a standardised curriculum that incorporates previous course content, to establish a shared knowledge baseline and enhance sustainability. However, this is not yet formally mandated.

Thematic overlaps between CBMs 4 and 5 are frequent and intentional. These programmes also impart knowledge relevant to other CBMs, such as CBMs 7 and 8. The OAS plays a valuable role in translating global discussions and decisions into practical, region-specific projects, thereby enabling broader and more inclusive participation in the cyber diplomacy ecosystem. CBM 4 efforts are further complemented by numerous national and globally funded capacity-building projects, which often operate on a shorter-term basis and benefit from

[215] Find an example here.

[216] OAS as part of open, informal, cross-regional group (2025): Non-Paper on Inter-regional Cooperation. The Role of Regional Organizations in Implementing the UN Framework for Responsible State Behaviour in Cyberspace.

[217] OAS CICTE (2022): Presentation. OAS/CICTE experiences related to the development and implementation of (a) inter-governmental Points of Contacts directories in the area of ICT security, and (b) other confidence building measures relating to ICT security.

external funding. While these initiatives do not require permanent structures, they significantly contribute to improving cyber maturity across the region. Taken together, it becomes clear that much of CBM 4's implementation occurs implicitly through these wide-ranging activities.

The annual working group meetings provide a platform for regular exchange and coordination on these efforts. To further promote transparency and track implementation, the web portal serves as a central platform listing workshops and trainings. Currently undergoing an overhaul, the portal will soon include statistics on participation per state and gender balance, linking CBM 4 with the objectives of CBM 7.

CBM 5

CBM 5 (2019): *"Encourage the incorporation of cybersecurity and cyberspace issues in basic training courses and training for diplomats and officials at the Ministries of Foreign Affairs and other government agencies."*

Background: CBM 5 calls on states to integrate cybersecurity and cyberspace issues into the basic training of diplomats and government officials, particularly within MFAs.[218] It addresses two region-specific needs: the ongoing demand for foundational knowledge and capacity-building (linked to CBM 4), and, echoing the rationale of CBM 3, the need to firmly establish cybersecurity as a foreign policy priority rather than a purely technical issue. This measure recognises the cyber domain as a strategic and diplomatic concern requiring informed engagement across government.[219] By embedding cyber diplomacy into official training structures, states can build long-term institutional knowledge, ensure coherence in external messaging, and strengthen their overall foreign policy apparatus. At the same time, it facilitates broader participation in global cyber diplomacy and serves as a translation mechanism between international discussions and regional realities.

Practice: This CBM outlines primarily national-level steps, with implementation varying significantly across member states. Some have institutionalised cyber diplomacy by appointing cyber diplomats or ambassadors – like Brazil and the Dominican Republic – and embedding the issue within their national security

[218] OAS CICTE (2024): Presentation. Secretariat of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace.

[219] OAS CICTE (2019): Draft Regional Confidence-Building Measures (CBMs) to Promote Cooperation and Trust in Cyberspace. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.12/19 rev. 2.

architectures,[220] while others remain at earlier stages, reflecting the region's diverse levels of cyber maturity. As with CBM 4, this measure is supported by the Cyber Diplomacy Training Program and a range of OAS-led workshops and masterclasses.[221] The boundaries between CBMs 4 and 5 are intentionally fluid and overlapping. One idea in this regard, is the development of a standardised regional curriculum for diplomats and officials across MFAs and relevant agencies, designed to establish a consistent knowledge base throughout the region.[222] Its mandate is still pending, however, signalling ongoing **implementation, but not widely**. Support from international partners and more cyber-mature states, particularly Canada and the United States, has also reinforced training and capacity-building efforts. Finally, the annual Working Group Meetings continue to provide a forum for states to exchange updates, best practices, and lessons learned.

CBM 6

CBM 6 (2019): *"Foster cooperation and exchange of best practices in cyber diplomacy, cybersecurity and cyberspace, through the establishment of working groups, other dialogue mechanisms and the signing of agreements between and among States."*

Background: CBM 6 encourages OAS member states to actively collaborate through the formation of specialised working groups and dialogue platforms focused on cyber diplomacy and cybersecurity challenges. By promoting the signing of agreements and the exchange of best practices, the measure aims to build mutual understanding, improve coordination in responding to cyber threats, and foster a cooperative environment. Such measures contribute to institutionalising ongoing dialogue, and efforts to enhance collective cyber stability.

Practice: This CBM is closely linked to CBM 5, with its objective of exchanging best practices on cyber diplomacy, cybersecurity, and cyberspace supported by the Cyber Diplomacy Training Program. Each Working Group meeting contributes to this goal by including sessions for lessons learned and sharing best practices. Additionally, the OAS member states' CSIRT network, financially supported by Canada and the United States, implicitly supports this CBM by building a network promoting the exchange of information on cybersecurity threats.

[220] Just to give two examples, read more on it here.

[221] OAS CICTE (2024): Presentation. Working Group on Cooperation and Confidence-Building Measures in Cyberspace.

[222] OAS CICTE (2024): Report of the Fifth Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.14/24.

In 2025, OAS member states also began holding meetings on the sidelines of the OEWG to coordinate and exchange information. Moreover, states engage in open, informal groups at the UN OEWG; for example, Brazil, Canada, Chile, Colombia, the Dominican Republic, and Uruguay are part of the Confidence Builder Group, Chile and Colombia are part of a group focusing on gender, Canada and Chile coordinated inputs regarding stakeholder participation in the UN processes, and the CICTE Secretariat engaged in inter-regional cooperation regarding the role of regional organisations in the implementing the UN framework for responsible state behaviour in cyberspace.

Some states actively link meetings or exercises they participate in to the implementation of this CBM, for instance an expert meeting between Mexico and the United States in 2023 on cyber strategy and workforce development or member states virtually participating in a conference.[223] However, since no formal agreements or dedicated working groups currently exist specifically for this CBM, its implementation remains largely implicit. Thus, CBM 6 is **implemented, but not widely**.

CBM 7

CBM 7 (2022): *"Encourage and promote the inclusion, leadership, and effective and meaningful participation of women in decision-making processes linked to information and communication technologies by promoting specific actions at the national and international levels, with the aim of addressing dimensions around gender equality, and the reduction of the gender digital divide, in line with the women, peace, and security agenda."*

Background: As of 2024, women accounted for only 20-24% of the cybersecurity workforce in Latin America and the Caribbean.[224] They also face barriers to digital inclusion, with lower levels of internet access, less training in digital technologies, and reduced confidence in their tech skills.[225] This CBM directly addresses this gender imbalance, targeting not only technical roles but also policy and decision-making positions. The rationale is clear: underrepresentation can lead to technologies that reflect the biases and blind spots of a limited demographic, potentially perpetuating gender disparities and even gender-based violence. Promoting gender diversity in cybersecurity therefore enhances fairness, builds

[223] Find these activities linked to the implementation of this CBM here.

[224] ISC2 (2024): Women in Cybersecurity: Inclusion, Advancement and Pay Equity are Keys to Attracting and Retaining More Women.

[225] BID (2022): La dimensión de género en la transformación digital empresarial de América Latina y el Caribe.

safer and more inclusive digital systems,[226] and contributes to sustainable peace,[227] aligning with the "Women, Peace, and Security Agenda."

Practice: The OAS collaborates with non-profit organisations such as WOMCY and LATAM Women in Cybersecurity, facilitating research like diagnostic studies on the status of women's inclusion in the cybersecurity sector[228] and capacity-building initiatives to close the regional skills gap and encourage greater female participation,[229] thereby engaging over 2,000 women in cybersecurity exercises.[230] With support from Canada, it also launched two diversity-focused initiatives: the "Creating a Cybersecurity Pathway program," which introduced cybersecurity fundamentals and career opportunities to over 500 young people across the Americas and the Caribbean, and the "Cyber Women Challenge," which has trained over 1,900 women between 2018 and 2023 to strengthen workforce diversity and build inclusive responses to cyber threats. The "Women in Cybersecurity Empowerment Network" created a platform for more than 800 women working in cybersecurity.[231] The OAS has also cooperated with UNIDIR on the publication "A Novel Approach to the 11 UN Norms for Responsible State Behaviour in Cyberspace: Guidelines for Gendered Implementation," which provides recommendations for gender-responsive application of the norms, linking CBM 7 with CBM 9.

At the international level, the "Women in International Security and Cyberspace (WIC)" Fellowship, organised and sponsored by Australia, Canada, the Netherlands, New Zealand, the United Kingdom, the United States, and Germany, has increased the participation and skills of women from Argentina, Chile, Colombia, and Ecuador, among others, in UN cyber diplomacy negotiations.[232] While not created under this CBM, it aligns closely with its objectives. In parallel,

[226] Brown, Deborah and Pytlak, Allison (2020): Why Gender Matters in International Cyber Security. Women's International League for Peace and Freedom and the Association for Progressive Communications.

[227] O'Reilly, Marie, Súilleabháin, Andrea, and Paffenholz, Thania (2015): Reimagining Peacemaking: Women's Roles in Peace Processes.

[228] Find more information on such an upcoming research project here.

[229] OAS (2024): Press Release. The OAS and WOMCY Partner to Promote the Participation of Women from the Americas in the Cybersecurity Sector. // Thorpe, James (2020): Latin America, Cybersecurity and women, how things are evolving.

[230] OAS (n.d.): Cybersecurity Program.

[231] Millar, Katharine and Ferrari, Verónica (2025): A Novel Approach to the 11 UN Norms for Responsible State Behaviour in Cyberspace: Guidelines for Gendered Implementation. // OAS (2022): Presentation of the Organization of American States on experiences in the area of capacity-building in the field of information and communications technology (ICT) security. Statement at the OEWG.

[232] See more on it here.

states like Chile and Colombia have highlighted gender equality in OEWG sessions, for example through their involvement in a cross-regional group on gender.[233] Moreover, Chile has integrated gender considerations into its national cybersecurity policy, while Canada addresses gender equality and cybersecurity in its National Action Plan on Women, Peace and Security.

Although many of these initiatives were not explicitly designed to fulfill this CBM, they implicitly advance its goals by fostering greater inclusion and gender equality in cybersecurity. CBM 7 therefore represents a formal commitment by states to strengthen women's participation in the field, while also prompting explicit actions. Implementation is further supported by the Cyber Diplomacy Training Program, which helps empower women to take on meaningful roles in cyber policy and practice.[234] Looking forward, the redesigned web portal will include tools to track women's participation in training programmes, enhancing transparency and accountability.

Working Group Meetings also provide an important platform for states to share progress; for example, during the fifth meeting, the Dominican Republic reported efforts to strengthen its cyber diplomacy capacity with a focus on gender inclusion. That meeting even dedicated a session to "Encouraging and Promoting the Inclusion, Leadership, and Effective and Meaningful Participation of Women in Decision-Making Processes Linked to ICTs," reaffirming the region's collective commitment to advancing gender equality in cyber governance.[235] Overall, this CBM is **implemented, but not widely**.

CBM 8

CBM 8 (2022): *"Promote study, discussion, development, and capacity-building at the national and international levels regarding the application of international law to the use of information and communications technologies in the context of international security by promoting voluntary exchanges of positions and national vision statements, opinions, legislation, policies, and practices on the subject, in order to promote common understandings."*

[233] See for example in this working paper on "Gender and the Future Permanent Mechanism", which is drafted and/or cosponsored amongst others by Chile, Colombia, Canada, Mexico, and Uruguay.

[234] OAS CICTE (2024): Presentation. Working Group on Cooperation and Confidence-Building Measures in Cyberspace.

[235] OAS CICTE (2024): Fifth Meeting of the Working Group on Cooperation and Confidence-Building Measure in Cyberspace. Agenda. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.7/24 rev. 1.

Background: Since 2013 (via the Group of Governmental Expert (GGE) report), the applicability of international law to cyberspace has been formally recognised,[236] providing binding guidelines for how states use and regulate ICTs, including their defense against malicious cyber operations. However, no universal consensus exists yet on how exactly international law applies in this domain, prompting more and more states to publish their own national positions. Against this backdrop, this CBM seeks to promote dialogue and capacity-building in the application of international law to the use of ICTs in the context of international security. It encourages states to voluntarily share their legal interpretations, policies, and practices in order to foster transparency, predictability, and mutual understanding. By clarifying national perspectives and potential red lines, this CBM helps reduce uncertainty, prevent miscalculation, and lower the risk of escalation in the cyber domain.[237]

Practice: This CBM responds to an expressed need from states in the region to receive support in developing national positions on the application of international law in cyberspace.[238] Implementation is advanced through the OAS Cyber Diplomacy Training Program,[239] Canada-supported webinars (with 22 member states already engaged in 2023),[240] and upcoming masterclasses for government officials on legal frameworks. The CICTE Secretariat also provides informal briefings and integrates the issue into Working Group discussions, and is further integrated in these meetings, for example, via the dedicated panel on "Exploring the Development of National Positions on the Applicability of International Law to Cyberspace."[241]

Unlike the African Union's regional approach,[242] the OAS framework encourages each state to develop its own position while acquiring the necessary legal and

[236] UN General Assembly, Group of Governmental Experts (2013): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Note by the Secretary-General. A/68/98. UN.

[237] Mačák, Kubo, Dias, Talita, and Kasper, Ágnes (2025): Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for State. CCDCOE. // Egan, Brian (2017): International Law and Stability in Cyberspace. In: Berkeley Journal of International Law 35 (1), p. 169-180. // Raleigh, Kimberly (2025) during the panel discussion at the 5th Working Group Meeting: "Without such positions, it is challenging for other states to understand where red lines are drawn and to avoid crossing them." (OAS CICTE (2024): Report of the Fifth Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace.)

[238] e.g., Chile and Colombia at the 3rd Working Group Session (OAS CICTE (2021): Report of the Third Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace.

[239] OAS CICTE (2024): Presentation. Working Group on Cooperation and Confidence-Building Measures in Cyberspace.

[240] e.g. course on international law of cyber operations in 2022 and course on the application of international humanitarian law to cyber operations in 2023, see here.

[241] OAS CICTE (2024): Agenda. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.7/24 rev.1.

[242] Common position of the African Union (2024).

institutional capacities. Several member states, including Brazil,[243] Canada,[244] Colombia,[245] Costa Rica,[246] and the United States,[247] have already published national positions and actively share best practices, while others are still developing theirs. The CICTE Secretariat, in collaboration with partners like Chatham House and UNIDIR,[248] has supported two states in this process so far through tailored regional dialogues and will continue to offer this assistance in an even more advanced way, which has been met with strong interest. Such support includes actor mapping, targeted webinars, in-person workshops, and inter-agency consultations to ensure institutional buy-in and national ownership. Thus, this CBM is **implemented, but not widely** yet, with more efforts on the way. However, it is important to emphasise that states are not developing a position on the application of international law in order to fulfill this CBM. Rather, CBM 8 describes a commitment to do so, and the implementation of the CBM supports the process by facilitating exchange, discussion, and support through capacity-building.

Moreover, this CBM seeks to promote the transparent exchange of views on areas of convergence and divergence among national positions within the region. For example, experts note that while Brazil and Costa Rica both consider sovereignty to be a binding rule that can be violated by cyber operations, they diverge in their interpretations of what specific actions would constitute a violation of sovereignty.[249] Although not originally developed under the framework of this CBM, the OAS Inter-American Judicial Committee's "Improving Transparency"-initiative offers a valuable foundation for such exchanges. Launched in 2018, the project aims to identify areas of convergence and divergence among states in the region regarding the application of international law to cyberspace. Drawing on questionnaires and expert meetings, including representatives of the member states, this initiative has produced five reports addressing key legal issues to create a baseline for further dialogue.[250] As a result, the project also emphasises the need for legal capacity-building to engage in relevant international legal dialogues, highlighting a regionally-specific need.[251]

[243] National position of Brazil (2021).

[244] National position of Canada (2022).

[245] National position of Colombia (2025).

[246] National position of Costa Rica (2021).

[247] National position of the United States of America (2020).

[248] see here.

[249] Hurel, Louise Marie (2025): Cyber Diplomacy in Latin America. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James: A Handbook for the Practice of Cyber Diplomacy.

[250] Find the reports here.

[251] Hollis, Duncan, Vila, Ben, Rakhlina-Powsner, Daniela (2020): Elaborating International Law for Cyberspace.

CBM 9

CBM 9 (2022): *"Promote the implementation of the 11 voluntary, non-binding norms on responsible State behavior in cyberspace adopted by resolution 70/237 of the General Assembly of the United Nations and promote reporting on these efforts taking into account the national implementation survey."*

Background: This CBM encourages member states to adopt and implement the 11 voluntary, non-binding UN norms of responsible state behaviour in cyberspace, first developed by the GGE[252] and further advanced through the OEWG. These norms guide states in promoting peace, security, and stability online, including commitments such as refraining from harming critical infrastructure, cooperating on the investigation of malicious cyber activity, and strengthening supply chain security. The CBM also calls on states to report national implementation efforts – using tools like the UNIDIR implementation survey – to enhance transparency, build trust, and identify regional capacity-building needs. In doing so, it aligns OAS efforts with global UN processes while translating them into concrete regional action.[253]

Practice: Within the framework of the OAS CBMs, the Cyber Diplomacy Training Program plays a key role through its masterclasses and webinars in supporting implementation by helping to interpret and contextualise these global norms for regional actors.[254] Implicit implementation also occurs through the participation of member states in the OEWG.[255] For states with limited resources to engage directly in UN processes, the OAS Working Group provides a crucial platform to receive updates, coordinate positions, and prepare joint statements, thereby strengthening regional coherence and visibility in global cyber diplomacy.

CBM 9 also mandates the CICTE Secretariat to assist states in implementing the 11 voluntary norms endorsed by the UN GGE and OEWG.[256] In practice,

[252] UN General Assembly (2015):Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Note by the Secretary-General. A/70/174.

[253] OAS CICTE (2023): Fourth Substantive Session of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025. Remarks of the Inter-American Committee against Terrorism.

[254] OAS CICTE (2024): Presentation. Working Group on Cooperation and Confidence-Building Measures in Cyberspace.

[255] see Mexico's update at the third meeting of the working group (OAS CICTE (2021): Third Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace. OAS/Ser.L/X.5. CICTE/GT/MFCC-23/21.)

[256] OAS CICTE (2021): Third Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace. OAS/Ser.L/X.5. CICTE/GT/MFCC-23/21.

many OAS CCB activities contribute to this effort implicitly. Specifically, the PoC Directory (CBMs 2 and 3), for example, makes a particular contribution to the implementation of norm a (interstate cooperation on security), norm b (consider all relevant information), norm c (prevent misuse of ICTs in your territory), and norm h (respond to requests for assistance).[257] Moreover, the CBM explicitly refers to the National Survey of Implementation of United Nations Recommendations on the Responsible Use of ICTs by States in the Context of International Security. This survey tracks national implementation, but it also asks to identify challenges to implementation and/or specific gaps in capacity-limiting implementation. It thereby serves as a baseline assessment tool, allowing UN member states to conduct regular self-assessments of the national implementation of recommendations and to track their progress. The shared results of the survey flow into the national profiles on UNIDIR's Cyber Policy Portal, thereby fostering transparency. However, it is not publicly known who shared information by using this survey.

Overall, the CBM is **implemented, but not widely** when it comes to explicit activities. However, this CBM is better understood as reflecting a broad commitment by member states to implement these norms, even though the absence of a universally agreed definition of implementation leaves each state to interpret and apply the norms through diverse and often complex national processes. This lack of a common framework makes it especially challenging to assess the extent of implementation.

CBM 10

CBM 10 (2022): *"In the sphere of information and communication technologies, promote work and dialogue with all stakeholders, including civil society, academia, the private sector, and the technical community, among others."*

Background: This CBM promotes a multi-stakeholder approach to cybersecurity, fostering inclusive dialogue and cooperation among governments, civil society, academia, the private sector, and the technical community. With much of the digital infrastructure privately owned and private companies often being the primary targets of malicious activity, their involvement is indispensable. At the same time, civil society and academia contribute by advancing awareness, supporting capacity-building, guiding the implementation of responsible state

[257] OEWG Chair (2025): Annex I: Voluntary Checklist of Practical Actions for the implementation of voluntary, non-binding norms of responsible State behaviour in the use of ICTs. In: Rev. 1 draft of the Final Report of the OEWG.

behaviour, and helping to share cyber threat intelligence.[258] Bringing these diverse perspectives together not only strengthens the effectiveness and sustainability of cybersecurity policies but also builds transparency, trust, and shared responsibility.

Practice: So far, CBM 10 has not been a primary focus with explicit activities taking place. However, there has been implicit **implementation, but not widely**. States have used the Working Group meetings to share updates on their national engagement with diverse stakeholders, and related panel discussions have been held in this context. Given its broad scope, CBM 10 can also be understood as an affirmation of the multistakeholder approach, underscoring the importance of inclusive dialogue and collaboration in cybersecurity. Notably, Chile and Canada have actively promoted the participation of non-state stakeholders within the OEWG, setting an implicit example of how this CBM's objectives can be advanced. In addition, the OAS has already established strong links with private sector actors and civil society,[259] providing a foundation that could be further leveraged to strengthen implementation moving forward.

CBM 11

CBM 11 (2022): *"Develop national cyber incident severity schemas and share information about them."*

Background: This CBM encourages member states to develop and share national cyber incident severity schemas – frameworks that classify incidents by impact, scope, and urgency[260] that enable authorities to assess and respond to incidents consistently and proportionately while helping prioritise resources. Sharing them across states fosters common understanding and interoperability, supporting faster, more coordinated cross-border responses and reducing the risk of misinterpretation or escalation caused by differing threat perceptions. In addition, it promotes transparency and facilitates information sharing and cooperation, which is particularly critical when incidents have transnational effects.[261]

Practice: Unlike many other CBMs, this measure has a clear and verifiable objective. At the fourth Working Group meeting, the United States presented

[258] Ciglic, Kaja, and Hernig, John (2021): A multi-stakeholder foundation for peace in cyberspace. Journal of Cyber Policy 6 (3), p. 360-274.

[259] OAS (2022): Presentation of the Organization of American States on experiences in the area of capacity-building in the field of information and communications technology (ICT) security.

[260] CISA (n.d.): National Cyber Incident Scoring System.

[261] OAS CICTE (2022): Concept Paper. CICTE/GT/MFCC/doc.3/22.

its cyber incident severity scoring system,[262] which is now being explored as a potential model for regional adoption. While the original plan envisioned each state developing its own schema and sharing it through the web portal,[263] discussions have shifted toward creating a common, standardised system to enhance interoperability and streamline information sharing. Efforts have not yet begun, so there is **no implementation**, but the CSIRTs Americas Network is expected to play a central role in moving this effort forward.

4.2.3. OAS moves to strengthen implementation efforts

The implementation of cyber CBMs within the OAS remains in its early stages. While notable progress has been made, much of the work still focuses on building the foundations for future action. Member states have recently agreed not to develop new cyber CBMs but to instead concentrate on the gradual, step-by-step implementation of the 11 existing CBMs. This phased approach makes it possible to address each cyber CBM individually and clarify what concrete implementation entails. To guide this process, a work plan is currently being developed, and implementation efforts will increasingly be tracked through the OAS web portal,[264] which is being updated to enhance transparency and accountability.

Launched in 2021, the web portal already supports the implementation of CBMs 1, 2, and 3, while the Cyber Diplomacy Training Program contributes to CBMs 4, 5, 7, 8, and 9, illustrating the CBMs' interconnected nature and the central role of shared infrastructure. The CICTE Secretariat serves as a key driver of implementation, coordinating and facilitating activities in line with mandates from member states. This ensures political ownership, alignment with national priorities, and responsiveness to actual needs. The Secretariat raises awareness of cyber CBMs, fosters experience-sharing and dialogue, and provides targeted capacity-building support when requested. The CICTE Secretariat therefore provides the resources to enable member states to implement cyber CBMs.[265]

A review of implementation to date highlights a strong emphasis on capacity-building, reflecting the significant variation in cyber maturity levels across the region.[266] Many states continue to face resource constraints that limit

[262] CISA (n.d.): National Cyber Incident Scoring System.

[263] OAS CICTE (2022): Concept Paper. CICTE/GT/MFCC/doc.3/22.

[264] Some activities have already been tracked and linked to the according CBM here.

[265] OAS CICTE (2023): Remarks of the Inter-American Committee against Terrorism Organization of American States at the OEWG.

[266] Barrett, Kerry-Ann (2025): Cybersecurity and Its Influence on Traditional Diplomacy in the Americas. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James (Eds.): A Handbook for the Practice of Cyber Diplomacy. EU Institute for Security Studies.

their ability to prevent and respond to cyber threats effectively. The CICTE Secretariat is therefore working to design tailored, demand-driven support while also coordinating with other initiatives to avoid duplication, as seen in the implementation of CBM 8. Importantly, there is a strong collaborative spirit across the region, with member states working together on shared resources, for example, discussions on a unified cyber incident severity schema under CBM 11. The first three are more traditional CBMs, while others, such as CBMs 3 and 5, specifically position cybersecurity as a diplomatic issue for MFAs and help bridge regional and global discussions (CBMs 6, 7, 8, and 9). This interplay between the regional and global levels is a defining feature of the OAS approach. The UN GGE and OEWG processes have elevated awareness of cybersecurity as a relevant (diplomacy) issue for the region as well as the question of how the regional perspective can be incorporated into global processes, while the CBMs provide the CICTE Secretariat with a mandate to translate global commitments into tangible regional action. Some cyber CBMs also reinforce ongoing capacity-building initiatives, ensuring that regional efforts build on existing projects.

Overall, the 11 cyber CBMs function as a flexible portfolio of options that take into account the diversity of maturity levels among member states. For example, some have already articulated positions on the applicability of international law in cyberspace and can share best practices in this regard, others are developing them with targeted support, and many are still building the institutional capacity to do so. The cyber CBMs vary in specificity: some outline concrete, verifiable actions, such as sharing national strategies (CBM 1), nominating PoCs (CBMs 2 and 3), creating a cyber diplomacy curriculum (CBM 5), or establishing incident severity schemas (CBM 11), while others (such as CBMs 7, 9, and 10), are broader in scope and serve primarily as commitments to shared objectives. Overall, unlike traditional CBMs, which focus on avoiding direct conflict, OAS cyber CBMs are more oriented toward fostering dialogue, cooperation, and regional engagement in global cyber processes.

For several member states – particularly those with limited resources – the OAS remains one of the most important platforms for advancing cybersecurity cooperation and capacity development. The Working Group has therefore emphasised both regional progress and contributions to global cyber stability.[267] This is evident in the regular integration of UN process updates into Working Group discussions, as well as plans to align the OAS PoC Directory with the UN Global Directory. The annual meeting of the Working Group provides a key

[267] OAS CICTE (2024): Report of the Fifth Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace. OAS/Ser.L/X.5. CICTE/GT/MFCC/doc.14/24.

platform for monitoring progress, sharing experiences, and identifying challenges. The 2025 meeting, chaired by the Dominican Republic, and the 2026 meeting, chaired by Canada, will continue this role.

In preparation, the CICTE Secretariat surveys member states to assess obstacles, asking whether governments have a clear understanding of cyber CBMs, what challenges they face, and what types of support would be most useful.[268] While the implementation of cyber CBMs in the OAS is still evolving, clear structures, political commitment, and momentum are in place. Thus, the region is gradually moving from planning to practice.

4.3. ASEAN Regional Forum (ARF)

4.3.1. Formulation of ARF cyber CBMs

The ASEAN Regional Forum (ARF) is a platform for dialogue and cooperation on security issues in the Asia-Pacific region. Established in 1994, it aims to promote peace and stability through discussions on regional security challenges, confidence-building in multiple thematic areas, and preventive diplomacy. The ARF includes 27 participating states[269] composed of ASEAN nations, Asia-Pacific states, and external partners with interests in regional security. All of these states have "an impact on the peace and security of the 'geographical footprint' of key ARF activities."[270] Thus, states from Asia, North America, as well as Australia and the EU are part of ARF, making it a regional organisation with a very broad membership.

The ARF first formally acknowledged the importance of confidence-building in the cyber domain in 2012, when its Foreign Ministers issued a statement at the 19th ARF Ministerial Meeting. The statement highlighted the "need for further dialogue on the development of confidence-building and other transparency measures to reduce the risk of misperception, escalation, and conflict."[271]

[268] OAS CICTE (2024): Presentation - Secretariat of the Working Group on Cooperation and Confidence Building Measures in Cyberspace.

[269] ASEAN Member States: Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand, Timor-Leste, Vietnam / Non-ASEAN Members and ASEAN Dialogue Partners: Australia, Bangladesh, Canada, China, Democratic People's Republic of Korea (North Korea), European Union (EU), India, Japan, Mongolia, New Zealand, Pakistan, Papua New Guinea, Republic of Korea (South Korea), Russia, Sri Lanka, United States.

[270] In 1996 the ASEAN Regional Forum adopted criteria for participation which are related to commitment, relevance, gradual expansion, and consultations. Findmore here.

[271] ARF (2012): Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security.

Building on this momentum, the ARF adopted its first Work Plan on Security of and in the Use of ICTs in 2015. The purpose of the work plan is "to promote a peaceful, secure, open and cooperative ICT environment and to prevent conflict and crises by developing trust and confidence between states in the ARF region, and by capacity-building."[272] It pursues several objectives: developing and implementing CBMs, enhancing transparency, improving mutual understanding in the ICT domain, raising awareness of threats, strengthening the protection of critical infrastructure, and building regional capacity to counter cyber threats, including those linked to criminal or terrorist activities. To achieve these aims, the Work Plan identifies six focus areas for activities: cooperation, PoCs, cultural diversity, information sharing, capacity-building, norms, rules, and responsible state behaviour.[273]

Unlike some other regional organisations, the ARF has not codified a set of formal, numbered CBMs.[274] Instead, it uses the Work Plan as the guiding framework from which concrete implementation activities are derived. Each activity must be co-hosted by at least one ASEAN and one non-ASEAN member state, reinforcing ASEAN's central role in the ARF process. The co-hosts prepare a concept paper for the Open Ended Study Group on CBMs and the Inter-Sessional Meeting on ICTs Security, which must then be approved sequentially by the ARF Inter-Sessional Support Group on Confidence Building Measures and Preventive Diplomacy, ARF senior officials, and finally the ARF foreign ministers.

4.3.2. Implementation of ARF cyber CBMs

Proposed CBM activity #1:

"Establish an open ended Study Group on Confidence Building Measures to reduce the risk of conflict stemming from the use of ICTs. The Group will comprise ARF Members. The Study Group could submit consensus reports recommending confidence building measures, drawing on previous ARF discussions and reviewing relevant work in other regional and international forums, taking in account the suggested activities set out in this Work Plan."

[272] ARF (2015): ASEAN Regional Forum Working Plan on Security of and in the use of information and communications technologies (ICTs).

[273] Malaysia's Representative (2021): (8th meeting) Open-ended working group on Information and Communication Technology (ICT) - First Substantive Session (13-17 December 2021).

[274] Even though this is sometimes mentioned, or measures from time to time are referred to as, e.g. CBM 1.

Background: The idea of establishing a study group was to create a dedicated body tasked with recommending concrete CBMs aligned with the activities outlined in the Work Plan. Its responsibilities include organising workshops and seminars, as well as developing processes and procedures for information-sharing among ARF contact points to prevent ICT-related crises and to address the criminal or terrorist use of ICTs.[275]

Practice: To advance this initiative, the Open-Ended Study Group on Confidence-Building Measures (OESG on CBMs) was established in 2017 to reduce the risk of conflict stemming from the use of ICTs. Functioning as an expert body subordinate to the ARF Inter-Sessional Meeting (ISM) on ICTs Security, the OESG operates under specific mandates, guiding principles, and rules of procedure set out in its Terms of Reference (TOR).[276]

Each meeting is co-chaired by one ASEAN and one non-ASEAN ARF participating state; for example, the Philippines and Canada assumed this role in 2025. Since its inception, the group has convened twice annually, with one session held alongside the ARF ISM on ICTs Security, bringing together officials and experts from across the ARF membership. In this sense, the activity has been **widely implemented**.

OESG activities must avoid duplicating or contradicting initiatives pursued in other regional or global fora. The TOR also underscores the need to respect the varying comfort levels and capacities of participating states, meaning that all activities must be consensus-based. Once consensus is achieved, the proposed measures are submitted for approval at successive ARF decision-making levels.

Proposed CBM activity #2:

"Conduct workshops and seminars for ARF Participating Countries.

> *The focus of these workshops and seminars, which would support the work of the Study Group, could include the following:*
>
> *I.* *the voluntary sharing of information on national laws, policies, best practices and strategies as well as rules and regulations related to security of and in the use of ICTs as well as the procedures for this sharing of information;*

[275] ARF (2015): ASEAN Regional Forum Working Plan on Security of and in the use of information and communications technologies (ICTs).

[276] see here.

> II. *discussion exercises involving cooperation among ARF participating countries, on how to prevent incidents related to security of and in the use of ICTs becoming regional security problems;*
>
> III. *conduct of surveys on lessons learnt in dealing with threats to the security of and in the use of ICTs and creation of ARF databases on potential threats and possible remedies, taking into account the work that is already done in the commercial computer security sector and in the CERT community in this regard;*
>
> IV. *capacity building related to security of and in the use of ICTs and to combating criminal use of the internet;*
>
> V. *promotion of and cooperation in research and analysis on issues relevant to security of and in the use of ICTs;*
>
> VI. *discussion on rules, norms, and principles of responsible behaviour by ARF Participating Countries and the role of cultural diversity in the use of ICTs;*
>
> VII. *raising awareness for non-technical personnel and policy makers on threats in the use of ICTs and methods for countering such threats;*
>
> VIII. *measures to promote cooperation among ARF Participating Countries against criminal and terrorist use of ICTs including, inter alia, cooperation between law enforcement agencies and legal practitioners, possible joint task force between countries, crime prevention and information sharing on possible regional cooperation mechanism;*
>
> IX. *discussion on the terminology related to security of and in the use of ICTs to promote understanding of different national practices and usage;*
>
> X. *consideration of establishment of senior policy Point of Contacts between ARF Participating Countries to facilitate real time communication about events and incidents in relation to security of and in the use of ICTs of potential regional security significance;*
>
> XI. *consideration of establishment of channels for online information sharing on threats in ICT space, global ICT incidents and sources of ICT attacks threatening critical infrastructure, and development of modalities for real time information sharing (leveraging activities conducted by CERT networks).“*

Of these proposed measures, some have received more attention than others thus far:

Proposed activity X (also referred to as CBM#1):

"Establishment of ARF Points of Contact (POC) Directory on Security of and in the Use of ICTs"

Background: This measure seeks to strengthen real-time communication among ARF participating states to help prevent tensions and reduce the risk of conflict stemming from the misinterpretation of ICT security incidents. Its purpose is to establish clear coordination mechanisms within the ARF so that states know exactly whom to contact when concerns arise. To accommodate ARF members' diverse institutional frameworks, the directory allows states to nominate a single coordination PoC or multiple PoCs across different levels, such as diplomatic (e.g., MFA), technical (e.g., CERT/CSIRT), law enforcement, or national security and policy coordination (e.g., ministries of interior or home affairs).[277]

This measure is considered fundamental, as it enables more effective communication and connectivity between technical and policy/diplomatic levels, unprecedented in ARF's work on ICT security. It also serves as a cornerstone for the implementation of other CBMs.

Practice: The measure is co-sponsored by Malaysia and Australia, which first introduced the idea through a concept paper, building on the outcomes of their joint ARF Workshop on Cyber CBMs in 2014. That workshop, along with related exercises, including a tabletop simulation, demonstrated the practical utility of such a directory.[278] The process of achieving consensus was neither quick nor simple, but once approved, it has been **widely implemented** and steadily advanced by the co-sponsors since 2018.[279] By 2020, roughly half of ARF members had nominated PoCs,[280] and by 2024, that number had grown to 20 states.[281]

A standardised template guides nominations, requiring information such as the type of PoC (diplomatic, technical, etc.), seniority level (with senior officials to be contacted only in situations of regional security significance), institutional

[277] Australia and Malaysia (2018): Concept Paper (Revised). ASEAN Regional Forum (ARF) Points of Contact Directory on Security of and in the Use of Information and Communications Technologies (ICTs).

[278] Malaysia's Representative (2022): (7th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Second Substantive Session (28 March-1 April 2022).

[279] Australia's Representative (2022): (7th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Second Substantive Session (28 March-1 April 2022).

[280] Malaysia's Representative (2021): (8th Meeting) Open-ended working group on Information and Communication Technology (ICT) - First Substantive Session (13-17 December 2021).

[281] Co-Chair (2024): Co-Chairs' Summary Report of the 6th ARF ISM on ICTs Security.

affiliation, and personal details such as name, title, contact information, spoken languages, and availability.[282] Access to the Directory is restricted exclusively to ARF members. Over time, additional procedures were developed to facilitate its use.[283]

Participation remains entirely voluntary, as each state independently decides how to respond to incoming communications and what information to share. For example, states may choose to initiate consultations via diplomatic channels in response to an incident, mutually agreeing on the format, timing, location, and cost-sharing arrangements, and may even involve a third-party mediator if desired. States are encouraged to maintain records of all exchanges.

To ensure that the Directory remains functional, its entries are validated, updated, and recirculated at every Study Group meeting, as it is not hosted on a live web platform but distributed as a digital list.[284] Ping tests – carried out periodically by Malaysia and Australia – serve to verify communication channels at both the strategic and working levels.[285] In 2024, the first dedicated meeting of PoCs was convened,[286] and it was also announced that future ping tests are to be extended to senior-level officials.[287]

[282] Australia and Malaysia (2018): Concept Paper (Revised). ASEAN Regional Forum (ARF) Points of Contact Directory on Security of and in the Use of Information and Communications Technologies (ICTs).

[283] Australia and Malaysia (2019): Concept Paper (Revised). ASEAN Regional Forum (ARF) Points of Contact Directory on Security of and in the Use of Information and Communications Technologies (ICTs).

"Procedure for Inquiry:

1. Call or email the relevant point of contact and provide your name and affiliation.
2. Provide as much information as possible regarding the nature of the incident.
3. Ask for additional information about the incident and provide your contact information. Indicate time sensitivity as appropriate.
4. Nominate preferred channel of communication and nominate the agency within your country that will become the primary point of contact for this specific incident.

Procedure for Responding to an Inquiry:

1. Provide an immediate response to the ICT security incident query (if possible), or:
2. Inform the point of contact that you will look into the ICT security incident and follow up with additional information. Provide an estimated timeframe for a response, as appropriate; and
3. Agree on preferred channel of communication and nominate the agency within your country that will become the primary point of contact for this specific incident."

[284] Australia and Malaysia (2018): Concept Paper (Revised). ASEAN Regional Forum (ARF) Points of Contact Directory on Security of and in the Use of Information and Communications Technologies (ICTs).

[285] Malaysia's Representative (2021): (8th Meeting) Open-ended working group on Information and Communication Technology (ICT) - First Substantive Session (13-17 December 2021).

[286] ARF (2024): Presentation. ARF experiences in assisting states in the selection, nomination & onboarding PoCs to the ARF PoC Directory.

[287] Co-Chair (2024): Co-Chairs' Summary Report of the 6th ARF ISM on ICTs Security.

Proposed activity I (also referred to as CBM#2):

“Sharing of Information on Domestic Laws, National Policies, Best Practices and Strategies as well as Rules and Regulations”

Background: This measure is designed to enhance transparency through information sharing, for example, by providing updates on national postures, systems, and policies, thereby supporting the ARF Work Plan’s overall objectives. It falls under the priority area of “awareness building and exchange of best practices.”

Practice: The measure was introduced in 2018 through a concept paper by co-sponsors Japan and the Philippines. Since then, it has been partially implemented through exchanges at each Study Group and ISM meeting, where ARF participants sometimes share information on domestic laws, policies, strategies, and regulations related to ICT security, as well as the procedures governing their application.[288]

Information sharing also extends to the ARF Annual Security Outlook (ASO) – published since 2000 – which offers an overview of the Asia-Pacific security environment, with each member state contributing its perspectives and reporting national initiatives. In recent years, many submissions have begun to include cybersecurity-related content, such as new legislation, strategies, and capacity-building programmes. Although not originally tied to this activity, these contributions have nonetheless implicitly supported its implementation by fostering confidence, transparency, and mutual understanding.

In 2020, Malaysia and New Zealand proposed the development of an online resource – a dedicated repository for ARF documents, reports, draft proposals, and workshop presentations – to further strengthen transparency and information sharing. While the ARF already maintains a portal, the proposal suggested either expanding it or establishing a standalone platform.[289] To date, however, no decision has been made in this regard. Overall, there is **no sufficient data available** to assess implementation activities.

[288] Japan and the Philippines (2018): Concept paper. Sharing of Information on Domestic Laws, National Policies, Best Practices and Strategies as well as Rules and Regulations (CBM#2) (Annex 5).

[289] Co-Chair (2020): Co-Chairs’ Minutes. 5th ASEAN Regional Forum Open Ended Study Group on Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies.

Proposed activity XI (also referred to as CBM#3):

"Protection of critical infrastructures and consultations mechanism"

Background: This measure supports the priority area of "critical information infrastructure protection frameworks and mechanisms" by emphasising cooperation and information sharing. Its purpose is to reduce the risk of conflict arising from ICT use by strengthening awareness and building capacity around critical infrastructure (CI) protection. By fostering voluntary cooperation through preventive and consultative frameworks, the measure aims to prevent misunderstandings that could escalate into political or military tensions. It is not designed to resolve ongoing conflicts but to mitigate risks before they emerge, offering a practical avenue for collaboration. Other tools may be more suitable in cases where conflict has already occurred, other tools may be more suitable.[290]

Practice: The measure was introduced in 2018 through a concept paper written by Singapore and the EU that outlined two complementary dimensions: the "preventive side of the coin" and the "cooperative side of the coin."[291] On the preventive side, states are encouraged to take national steps such as defining baseline security requirements, establishing incident notification frameworks, and designating competent national authorities. For example, Singapore and the Netherlands shared their joint 2017 initiative to develop baseline IoT security standards, illustrating how such practices could inform regional discussions.[292] The measure also links to activity I, as information exchanged under that framework can help shape national and regional CI protection efforts.[293] In practice, some states have shared how they classify CI during annual meetings. Additionally, ASEAN's 2019 regional framework for identifying and protecting CI – though not formally part of this CBM – can be seen as implicitly relevant, offering methodologies, best practices, and strategic recommendations.[294] The concept paper also proposed regular working group meetings of CI operators from ARF states, but these have not yet materialised.

[290] Singapore and the EU (2018): Concept paper. Protection of Critical Infrastructures and Consultations Mechanism (CBM#3). (Annex 6).

[291] Singapore and the EU (2018): Concept paper. Protection of Critical Infrastructures and Consultations Mechanism (CBM#3). (Annex 6).

[292] Find the 2019 published study here.

[293] Singapore and the EU (2018): Concept paper. Protection of Critical Infrastructures and Consultations Mechanism (CBM#3). (Annex 6).

[294] See here.

On the cooperative side, the co-sponsors proposed a consultation mechanism designed to defuse the risk of misperception or escalation stemming from malicious ICT activity against CI. Under this mechanism, if one ARF member (the requesting party) experiences such an incident and suspects that another ARF member (the requested party) may be involved, it can issue a notification via the PoCs established under activity X. This notification is intended to initiate dialogue without attributing blame. The requested party is expected to acknowledge receipt promptly – ideally within 48 hours – and provide a timeline for response. The states may then pursue consultations through diplomatic channels, deciding by mutual agreement on the format, location, timing, and cost-sharing. Third-party mediation or observers may also be included. Consultations can be ended at any point by mutual consent, and unresolved cases may be escalated to the UN Security Council.[295] There is no record to date of it having been used.

Despite limited formal uptake, progress has been made through workshops: Singapore and the EU co-hosted a virtual event in 2021 on protecting ICT-enabled CI (due to the COVID-19 pandemic) and a follow-up workshop in 2024 on strengthening CI security and resilience. Both workshops were well attended and contributed to sustaining momentum around this measure. Thus, the measure is **implemented, but not widely**.

Proposed activity VII (also referred to as CBM#4):

"Awareness-raising and Information Sharing on emergency responses to security incidents in the use of ICTs"

Background: Using the WannaCry ransomware campaign[296] as an example, the concept paper for this measure[297] emphasised the importance of cooperation at the bilateral, regional, and international levels to effectively respond to ICT security incidents. Attribution challenges make this cooperation particularly critical, as uncertainty can heighten the risk of misperception and escalation. This measure

[295] Singapore and the EU (2018): Concept paper. Protection of Critical Infrastructures and Consultations Mechanism (CBM#3). (Annex 6).

[296] The 2017 WannaCry ransomware campaign spread rapidly across internal networks and the public internet by exploiting a vulnerability in Microsoft Windows. It used "EternalBlue," an NSA-developed exploit that had been leaked by the Shadow Brokers earlier that year. Within hours, the self-propagating worm had infected more than 200,000 systems in 156 countries, hitting critical infrastructure operators - including healthcare, energy, transport, finance, and telecommunications - alongside manufacturers and service providers. The attack caused hundreds of millions of dollars in damage and was later attributed to North Korea's Lazarus Group (APT38). (Mandiant (2017): WannaCry Malware Profile.)

[297] China (2018): Awareness-raising and Information sharing on emergency responses to security incidents in the use of ICTs. (Annex 7).

therefore focuses on strengthening cooperation and coordination in research among the ARF participating states in raising awareness, sharing information, and ensuring timely and appropriate responses to ICT-related incidents. It contributes to the priority area "Awareness Building and Exchange of Best Practices."

Practice: China first introduced this measure in 2018 through a concept paper, and was later joined by Cambodia and Singapore. Cooperation was envisioned through cross-border workshops bringing together diplomats, policymakers, law enforcement, technical experts, and academics, as well as tailored public-awareness campaigns adapted to each state's social, economic, and cultural context. Participating states were encouraged to exchange expertise among relevant agencies and provide technical training to the less-developed ARF members. In parallel, voluntary information sharing was to be facilitated through designated PoCs, common categories and formats for data exchange, and potentially, an ARF information-sharing platform to identify needs, circulate lessons learned, and support long-term cooperation.[298] This approach links closely to the PoC Directory described under activity X and also overlaps with activity V of the ARF Work Plan, which highlights the importance of joint research.

One workshop was held in Malaysia in 2020, attended by 45 participants from 15 ARF participating states. Discussions covered ICT incident response, awareness raising, best practices, and international cooperation.[299] Overall, there is **no sufficient data available** to assess implementation activities.

Additional proposed activity (also referred to as CBM#5):

"ASEAN Regional Forum Workshop On National Cybersecurity Strategy Building"

Background: As the cyber domain grows in strategic relevance, it is essential for states to establish clear national guiding principles in this regard that provide the basis for national strategies, helping states coordinate internal efforts, allocate resources efficiently, and ensure cohesive action across ministries and stakeholders – particularly in times of crisis. They also promote transparency, predictability, and trust at the regional level. This measure aims to facilitate discussions on how ARF members conceptualise and design strategies for ICT security in ways suited to their national contexts. It contributes to the priority area "Establishment of Coordination Mechanisms within the ARF."

[298] China (2018): Awareness-raising and Information sharing on emergency responses to security incidents in the use of ICTs. (Annex 7).

[299] Co-Chair (2020): Co-Chairs' Minutes. 5th ASEAN Regional Forum Open Ended Study Group on Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies.

Practice: Singapore introduced a concept paper in 2018 proposing a capacity-building workshop on cybersecurity strategy building. Canada later joined as a co-sponsor, and the two states hosted a workshop in Singapore in 2019. The event gathered over 30 senior officials from ASEAN states, Australia, China, Republic of Korea, Russia, Timor Leste, and the United States, with additional input provided by the OAS. Participants explored emerging cyber threat trends and frameworks for building national strategies, and took part in a simulation exercise on responding to a cyber operation. No further workshops on this specific topic have been held since.[300] Except for this, there is **no sufficient data available** to assess implementation activities.

Additional Implementation Efforts:

In addition to the measures and activities described above, further efforts are underway to advance the implementation of the activities proposed in the Work Plan:

Proposed activity IV: *"capacity building related to security of and in the use of ICTs and to combating criminal use of the internet"*

Workshops on this theme were facilitated under ARF auspices beginning in 2021.[301] The first was held virtually, followed by another in 2022 co-sponsored by Russia, China, and Viet Nam,[302] and a hybrid workshop in 2024 co-sponsored by Russia, China, and Thailand. Participants included government officials, private sector representatives, and academics, who discussed criminalisation, prevention, international cooperation, legal frameworks, and investigative practices. Some states voiced concerns about duplication with other ASEAN mechanisms, suggesting that the issue fit better under the ARF Counter-Terrorism and Transnational Crime workstream. Russia, however, emphasised that capacity-building on ICT-related crime falls squarely within the ARF's 2015 Work Plan on ICT Security.[303] This activity contributes to the priority area "Combating Criminal and Terrorist Use of ICTs."

Proposed activity VI: *"discussion on rules, norms, and principles of responsible behaviour by ARF Participating Countries and the role of cultural diversity in the use of ICTs"*

[300] Co-Chair (2020): Co-Chairs' Minutes. 5th ASEAN Regional Forum Open Ended Study Group on Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies.

[301] Find it here.

[302] See here.

[303] Co-Chair (2024): Co-Chairs' Summary Report of the 6th ARF ISM on ICTs Security.

In 2022, Indonesia and Australia co-sponsored a virtual workshop on "Rules, Norms, and Principles of Responsible Behaviour of States in their Use of ICTs," this could be tied to proposed activity VI.

Proposed activity IX: *"discussion on the terminology related to security of and in the use of ICTs to promote understanding of different national practices and usage"*

This activity seeks to address persistent challenges around terminology in the field of ICT security, with the aim of fostering common understanding and avoiding misperceptions.[304] Russia introduced a concept paper in 2020,[305] later joined by Cambodia, and hosted virtual workshops in 2022 and 2023.[306] Discussions underscored the need for shared terminology and highlighted the lack of a common glossary. In 2020, Russia also proposed creating a dictionary of basic ICT security terms, but this idea did not achieve consensus. While China supported it, others – including Australia and the United States – favoured exchanging national approaches instead of pursuing a single common terminology.[307] By 2024, a survey was conducted to collect states' inputs on terms used in legislation, doctrines, and practice.[308] This once again highlights the complex and contested nature of language in the cybersecurity domain.

4.3.3. Workshops as the ARF's primary tool for implementation

The ARF has pursued a distinctive approach to developing and implementing cyber CBMs that differs notably from other regional organisations. Whereas other regions often adopt a clearly defined set of cyber CBMs, the ARF's 2015 Work Plan instead provides a menu of potential thematic activities, without formally designating specific measures. Co-sponsoring states initiate and develop activities within this framework. The sponsorship model is informal: being listed as a co-sponsor signals interest rather than binding commitment, though sponsors are generally expected to assume some responsibility, including logistical and financial contributions. This dynamic naturally highlights which states are more engaged than others. All proposals require consensus and must pass through multiple

[304] Chairman (2022): Chairman's Statement of the 29th ASEAN Regional Forum.

[305] Co-Chair (2020): Co-Chairs' Minutes. 5th ASEAN Regional Forum Open Ended Study Group on Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies.

[306] Russian Federation (2023): Contribution of the Russian Federation to the report of the UN Office for Disarmament Affairs on national ICT security capacity-building programs and initiative.

[307] Co-Chair (2020): Co-Chairs' Minutes. 5th ASEAN Regional Forum Open Ended Study Group on Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies.

[308] Co-Chair (2024): Co-Chairs' Summary Report of the 6th ARF ISM on ICTs Security.

decision-making layers before implementation, which often results in a slow and cumbersome process. Over the years, many proposed workshops have been blocked, primarily due to geopolitical tensions and ideological divides.

In practice, nearly all implemented activities – apart from the PoC Directory (Activity X), which remains the most durable and institutionalised measure – have taken the form of one-off workshops. Since the adoption of the Work Plan, the ARF has conducted about one or two such workshops annually. External disruptions, including the COVID-19 pandemic and travel restrictions following Russia's war of aggression against Ukraine, further constrained implementation. While virtual and hybrid formats helped sustain momentum, they reduced opportunities for personal interaction – an essential element of trust-building.

Measured against the 2015 Work Plan, many proposed activities have at least been partially addressed. Activity 1 (establishing the OESG) has been fully realised, with the group meeting regularly. Under Activity 2, workshops have been held on themes corresponding to sub-items I, IV, VI, VII, VIII, IX, X, and XI, demonstrating broad thematic engagement, though several proposed activities remain unaddressed. While only a few workshops are planned for the coming two years, this already exceeds previous levels and is thus a positive development.

Unlike other regional organisations that employ a diverse set of instruments, such as joint exercises, technical exchanges, or shared platforms, the ARF deliberately chose workshops as its primary mode of implementation. While this approach has limitations, it aligns with the ARF's consensus-driven and inclusive structure and reflects the expectations set at the time of the Work Plan's adoption. The ARF maintains transparency by listing all workshops on its website, and within the ARF ASO framework, states also report on these activities, often adding perspectives and national initiatives on cybersecurity, thereby contributing to information exchange.

The ARF's broad and diverse membership is both an asset and a liability. On the one hand, it offers a unique forum for inclusive dialogue among actors that might otherwise have little opportunity to engage. On the other hand, geopolitical tensions frequently produce stalemates, undermining progress. These dynamics are dominant in the cyber domain, where consensus has been especially elusive.

Moreover, the ARF does not appear to be a high-priority platform for many of its members. ASEAN plays a more central and trusted role for Southeast Asian states in the cyber domain. Many capacity-building activities on various topics are being implemented within ASEAN's framework, including through the ASEAN Cyber

Capacity Programme and the ASEAN-Japan Cybersecurity Capacity Building Centre, and the implementation of the norms is also being further developed within this scope.[309] Since 2020, the ASEAN CERT Information Exchange Mechanism has held biannual sessions in which member states share threat intelligence, discuss incidents, and coordinate mitigation measures. Building on this foundation, ASEAN is in the process of establishing a regional CERT – funded and hosted by Singapore – with its taskforce convening for the first time in August 2024 under Malaysia's coordination.[310] The EU's engagement in the ARF is limited, represented only through the European External Action Service (EEAS), with minimal direct involvement of individual member states.

Although the ASEAN Secretariat hosts an ARF Unit, its mandate covers the forum's overall activities rather than provide dedicated support to the ISM on ICTs. As a result, the ARF remains less transparent and less institutionally equipped compared to other regional organisations.

At present, the ARF OESG on CBMs and the ARF ISM on ICT Security (currently, co-chaired by the Philippines and Canada) are seeking to revive implementation. Yet, the ARF as a whole stands at a crossroads. The forum is now exploring a transition into a phase of "preventative diplomacy"[311] amid growing geopolitical polarisation and persistent criticism of its slow and cumbersome processes,[312] including in the area of cyber CBMs.

4.4. United Nations (UN)

4.4.1. Formulation of UN cyber CBMs

The United Nations (UN), established in 1945 to uphold international peace, security, and cooperation, has progressively broadened its agenda to include cybersecurity. Acknowledging the growing impact of digital threats, it has

[309] For example in 2018, the ASEAN leaders expressed a commitment to operationalise the UN norms, as well as via the ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace published in 2025 and various workshops in this regard.

[310] Singapore as part of the OEWG Confidence Builders (2024): Joint Working Paper, How information sharing contributes to security and stability in cyberspace: Examples from Regional Points of contact networks.

[311] ARF (2024): ASEAN Regional Forum - Annual Security Outlook.

[312] Seng Tan, See (2019): Rejuvenating the ARF: Challenges and Prospects. In: CSCAP Regional Security Outlook + ARF the next 25 years. // Hassan, Mohamed Jahwar (2021): The ASEAN Regional Forum: Challenges and Prospects. // Simon, Sheldon (2013): The ASEAN Regional Forum - Beyond the Talk Shop?

engaged in shaping responsible state behaviour in cyberspace by setting up dedicated temporary working groups within the purview of the UN General Assembly's First Committee on Disarmament and International Security.

The Groups of Governmental Experts (GGE), with the first group convened in 2004, brought together a select limited number of UN member states (ranging from 15 to 25, depending on the iteration) to assess threats in the cyber domain and recommend measures to enhance international peace and security. Its substantive reports, inter alia, affirmed for the first time that international law, including the UN Charter, applies to cyberspace (2013) and introduced 11 voluntary, non-binding norms for responsible state behaviour (2015). Although the GGEs did not include full UN membership participation at the time, all reports were adopted by consensus and subsequently endorsed by the UN General Assembly (UNGA), thereby giving their outcomes universal recognition. Over the course of six iterations, the GGE played a pivotal role in shaping the global cyber stability framework before the last group's mandate concluded in 2021.[313]

In parallel, the first Open-ended Working Group (OEWG) was launched in 2019 offering a more inclusive, all-member-state platform. Building on the GGE's work, it rapidly became the primary multilateral platform for cyber discussions. A second five-year OEWG was established in 2020 and held 11 substantive sessions and multiple informal intersessional meetings. Like the GGE, its work was structured around six thematic pillars: existing and potential threats, norms of responsible state behaviour, applicability of international law, CBMs, capacity-building, and regular institutional dialogue. The OEWG successfully adopted three annual progress reports (APRs 2022, 2023, 2024) by consensus and concluded with consensus on a final report in July 2025.

This report encapsulated five years of negotiations and laid the foundation for a permanent UN mechanism: the "Global Mechanism on Developments in the Field of ICTs in the Context of International Security and Advancing Responsible State Behavior." The mechanism will ensure continued dialogue on international cyber stability, including the exchange and potential further development of CBMs.

The GGE reports were instrumental in introducing CBMs as a voluntary tool for managing cyber risks, with the 2013 and 2015 reports offering key recommendations on their design. Building on these, states reached consensus within the OEWG on eight voluntary CBMs: the first four were adopted in 2022-2023, followed by four more in 2024.

[313] The iterations took place in the following years: 2004/05, 2010, 2013, 2015, 2016/17, 2019/21.

These eight voluntary CBMs were reaffirmed as part of the framework's acquis in the OEWG's final report.

4.4.2. Implementation of UN cyber CBMs

CBM 1

CBM 1 (2022): *"Nominate national Points of Contact to the Global POC Directory, and operationalize and utilize the Global POC Directory."*

Background: This CBM invites the member states to nominate technical and diplomatic PoCs to take on different roles – also taken into account and complemented by the work of CERTs / CSIRTs. The Directory is designed as "voluntary, practical and neutral in nature, developed and implemented in accordance with the principles of sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States."[314] Its core purpose is to strengthen communication and cooperation among states. The Directory aims to support timely coordination during significant ICT incidents, reduce the risk of misunderstandings, and facilitate information-sharing and capacity-building to improve prevention, response, and recovery efforts.[315] This CBM is considered fundamental for the implementation of further measures and an enabler of effective cooperation in the capacity-building domain, particularly for information exchange.

Practice: The establishment of the Global PoC Directory was the result of a lengthy and complex process. The idea was introduced in the 2013 and 2015 GGE reports, which recommended that states nominate national PoCs. Over the years, through dedicated exchanges on how such a network could be organised, the proposal became more precise until, in the 2022 APR, states reached consensus to establish a global PoC Directory. This decision built on existing regional initiatives, recognising that not all states were part of regional PoC networks.[316] In 2022, states agreed to prioritise its development. The fourth and fifth substantive OEWG sessions focused on the next steps and operational design, complemented by an intersessional meeting in December 2022 dedicated exclusively to the

[314] Annex A of the second APR - UN General Assembly (2023): Developments in the field of information and telecommunications in the context of international security. (A/78/265).

[315] Annex A of the second APR - UN General Assembly (2023): Developments in the field of information and telecommunications in the context of international security. (A/78/265).

[316] As a basis for this, the CBM refers to the following section from previous reports: UN General Assembly (2022): Developments in the field of information and telecommunications in the context of international security. (A/77/275). (first APR, CBM section, Recommended Next Steps, paragraph 2).

Directory. In this context, capacity-building needs were discussed, alongside a background paper prepared by the UN Secretariat compiling states' views. To further inform implementation, UNIDIR conducted a study, published in 2023 on behalf of the OEWG, analysing existing PoC networks and collecting state inputs.

Member states agreed that the United Nations Office for Disarmament Affairs (UNODA) would maintain the Directory, and a secure, password-protected web platform was created for member states.[317] Importantly, the Directory itself does not store sensitive communications; instead, states engage through mutually agreed upon, potentially secure, bilateral channels. Agreed principles specify that the information exchanged should remain confidential, may only be shared with third parties with mutual consent, and should, where possible, be documented by PoCs. Clear operational procedures for initiating and responding to requests via the Directory were also defined.[318] Some states have suggested developing standardised templates to improve the clarity and timeliness of communications. While initial proposals have already been put forward,[319] they remain under discussion within the framework of the new global mechanism.

Since its launch in May 2024, participation has steadily expanded. UNODA has supported states through practical resources such as the guide "POC101: How to Access and Participate in the PoC Directory," tailored e-learning courses, and awareness-raising activities. By May 2024, 92 states had nominated PoCs[320] and by mid-2025, this number had risen to about 120 states,[321] with roughly 300 PoCs

[317] See here.

[318] Annex A of the second APR - UN General Assembly (2023): Developments in the field of information and telecommunications in the context of international security. (A/78/265).

"Procedure for inquiry:

1. Call or email the relevant point of contact and provide your name and affiliation.
2. Provide as much information as possible regarding the nature of the incident.
3. Ask for additional information about the incident and provide your contact information. Indicate time sensitivity as appropriate.
4. Nominate preferred channel of communication and nominate the agency within your country that will become the primary point of contact for this specific incident.

Procedure for responding to an inquiry:

1. Provide an immediate response to the ICT security incident query (if possible), or:
2. Inform the point of contact that you will look into the ICT security incident and follow up with additional information. Provide an estimated timeframe for a response, as appropriate; and
3. Agree on preferred channel of communication and nominate the agency within your country that will become the primary point of contact for this specific incident."

[319] Find the proposal of the UN Secretariat (2024) here.

[320] UNODA (2024): Presentation. The global intergovernmental points of contact directory as established by the OEWG ICT security.

[321] UNODA's Representative (2025): (5th meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025).

registered overall. Most states nominated both technical and diplomatic contacts, though some submitted only one category and others nominated several. To avoid duplication, many states opted to nominate the same PoCs used in regional networks. Discussions continue on how best to leverage these regional-global synergies. Thus, this CBM is **widely implemented**.

Biannual ping tests are conducted to ensure functionality: UNODA sends a message to all registered PoCs, who must confirm receipt within 48 hours.[322] In 2024, tests were held in June and December, yielding a 60-70% response rate.[323] States also receive an annual reminder to update PoC details, with updates accepted on a rolling basis.[324] Practical exercises further strengthen the Directory's use. In March 2025, the first virtual tabletop exercise was organised by the OEWG II's Chair, supported by UNODA, UNIDIR, and ITU.[325] It simulated the use of the Directory under different time-zone scenarios. In addition, voluntary PoC meetings were initiated, including a hybrid meeting in May 2024, to share experiences and lessons learned.[326]

This CBM is also linked to CBMs 5 and 6, as states noted that "networks and directories could serve as platforms for capacity-building and knowledge-sharing. Capacity-building activities such as training sessions, seminars and other initiatives were noted as useful for strengthening expertise, knowledge and cooperation, which would in turn allow for more effective engagement in the directory."[327] However, this also suggests that it is not yet entirely defined what the directory will be used for. At the same time, misuse of the directory has already been discussed.[328]

CBM 2

CBM 2 (2023): *"Continue exchanging views and undertaking bilateral, sub-regional, regional, cross-regional and multilateral dialogue and consultations between States."*

[322] UNODA (2024): POC 101: How to Access and Participate in the PoC Directory.

[323] Shared during the OEWG side event in 2025 on the "Global intergovernmental points of contact directory: Towards universal participation", see here.

[324] Find an example here.

[325] Find the note verbal on it here.

[326] Find more information on it here.

[327] UNODA (2024): Initial background paper on capacities required to participate in a global intergovernmental points of contact directory.

[328] France's Representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Ninth Substantive Session (2-6 December 2024). // Germany's Representative (2025): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025).

Background: This CBM was first articulated in its current form in the second APR (2023), building on earlier GGE and OEWG outputs. It emphasises the value of open and transparent exchanges on threat perceptions, vulnerabilities, responsible state behaviour, and good practices, with the aim of broadening perspectives and improving state preparedness, including early warnings of emerging threats. This CBM also encourages the exploration of mechanisms for regular cross-regional exchanges of lessons learned and good practices related to CBMs. It underscores the importance of considering CBMs at the bilateral, regional, and multilateral levels, while recognising regional differences and the institutional structures of relevant organisations. Ultimately, the measure seeks to advance the collective development and implementation of the framework for responsible state behaviour in the use of ICTs, while enhancing transparency and predictability of state behaviour in cyberspace.[329]

Practice: This CBM is broadly formulated, encompassing a wide spectrum of activities. Member states often stress that the OEWG itself functions as a CBM by providing a platform for regular exchanges of views on threats, responsible state behaviour, and the implementation of CBMs. This is particularly relevant in the context of CBM 2 and contributes significantly – albeit implicitly – to its implementation. Even though such exchanges are sometimes criticised for remaining surface level,[330] the very fact that they take place in an inclusive, multilateral setting is seen as a success. The aim of this CBM is to continue fostering such exchanges, highlighting the spirit that "the OEWG itself served as a CBM."[331] This function could be carried forward under the future Global Mechanism: "States highlighted that the future permanent mechanism could likewise serve as a CBM as well as a platform for the implementation of CBMs."[332]

Overall, this CBM can be understood as one that may not necessarily require explicit activities for its implementation but that is primarily realised through ongoing dialogue and engagement. At present, there is no clearly defined global vision for what its implementation should concretely entail. Nevertheless, an open, informal, cross-regional group of states ("Confidence Builders" consisting of Australia, Brazil, Canada, Chile, Colombia, Czech Republic, Dominican

[329] OEWG Confidence Builders (2023): Joint Working Paper. Building Confidence and Capacity in a Cyber Way.

[330] Lewis, James (2025): The Practice of Cyberdiplomacy. In: Salvi, Andrea, Tiirmaa-Klaar, Heli, Lewis, James (Eds.): A Handbook for the Practice of Cyber Diplomacy. EU Institute for Security Studies.

[331] As a basis for this, the CBM refers to the following section from previous reports: UN General Assembly (2022): Developments in the field of information and telecommunications in the context of international security. (A/77/275). (first APR, paragraph 16 (e)).

[332] UN General Assembly (2025): Draft Final Report (A/AC.292/2025/CRP.1).

Republic, Fiji, Ghana, Germany, Israel, Jordan, Republic of Korea, Mexico, The Netherlands, Singapore, Uruguay) has put forward suggestions to shape its future implementation: "States should consider using existing dialogues and fora to voluntarily share information and good practices, lessons or white papers on existing and emerging ICT security-related threats and incidents, national strategies and standards for vulnerability analysis of ICT products, national and regional approaches to risk management and conflict prevention and national approaches to classifying ICT incidents in terms of scale and seriousness."[333] These proposals demonstrate that this CBM's implementation is linked to CBMs 3 and 4.

While no explicit global implementation measures have yet been adopted, implicit progress can already be observed through activities within the OEWG and related fora. Thus, this CBM is **implemented, but not widely**. Nevertheless, the CBM's practical application remains somewhat undefined, and its future development will likely depend on the extent to which states are willing to operationalise these proposals under the Global Mechanism.

CBM 3

CBM 3 (2023): *"Share information, on a voluntary basis, such as national ICT concept papers, national strategies, policies and programmes, legislation and best practices, on a voluntary basis."*

Background: This CBM was first articulated in its current form in the second APR in 2023. Building on earlier reports, CBM 3 is designed to foster transparency and predictability among UN member states. It encourages states to openly share their strategic objectives, priorities, governance structures, and national cybersecurity policies, for example, through concept papers, national strategies, laws, and programmes, as well as information on ICT institutions with relevance to international security.[334] By doing so, states can anticipate each other's actions and policies in the cyber domain, reducing the risk of misperceptions and helping organisations and agencies make effective risk management decisions.[335]

[333] OEWG Confidence Builders (2023): Joint Working Paper. Building Confidence and Capacity in a Cyber Way.

[334] As a basis for this, the CBM refers to the following section from previous reports: UN General Assembly (2022): Developments in the field of information and telecommunications in the context of international security. (A/77/275). (first APR, Recommended Next Steps, paragraph 5).

[335] OEWG Confidence Builders (2023):Joint Working Paper. Building Confidence and Capacity in a Cyber Way.

Practice: This CBM is deliberately broad, allowing states to pursue multiple avenues for information-sharing. One channel is the submission of reports to the UN Secretary-General, which may include national assessments, lessons learned, good practices on CBMs, or broader developments in ICTs in the context of international security.[336] Another option states may use is the UNIDIR Cyber Policy Portal (CPP)[337] – launched in 2019[338] – which maps the cyber policy landscape of all 193 UN member states, alongside major intergovernmental organisations and multi-stakeholder initiatives. By the end of 2023, the portal included over 1,500 documents, either submitted directly by states or collected by UNIDIR from official public sources.[339] Initially conceived as an information hub, the CPP has since evolved into a confidence-building tool, supporting the implementation of this CBM by enabling transparency and comparability. It also integrates data from the National Survey of Implementation of United Nations Recommendations on the Responsible Use of ICTs by States in the Context of International Security. This survey tracks state implementation of recommendations from the 2015 GGE report (and later OEWG/GGE outputs), while also identifying challenges and capacity gaps. The results feed into the CPP as a baseline assessment tool (also referenced in regional CBMs, such as OAS CBM 9). While states may choose to publicise their survey results, to date only the Czech Republic has done so. It should be noted that the CPP predates this CBM's formal adoption and now serves as a central instrument for its implementation.

In addition, the OEWG has become a venue where states share their cybersecurity objectives, priorities, and governance structures. For example, Australia, as part of the Confidence Builders group, contributed a joint working paper showcasing national strategies, white papers, and progress reports as practical inputs to this

[336] As a basis for this, the CBM refers to the following section from previous reports: UN General Assembly (2021): Developments in the field of information and telecommunications in the context of international security. (A/AC.290/2021/CRP.2). (Paragraph 48).

[337] The Cyber Policy Portal is maintained by UNIDIR's Cyber Stability workstream, part of its Security and Technology Programme, and is supported by voluntary contributions from the governments of the Czech Republic, France, Germany, Italy, the Netherlands, Switzerland, the United Kingdom, and Microsoft. It traces its origins back to UNIDIR's "2013 Cyber Index: International Security Trends and Realities", which initially sought to provide a comprehensive overview of national, regional, and international cyber activities during a time of rapid policy development. This early work highlighted the need for a continuously updated digital resource, and eventually gave rise to the CPP. The Portal is available in all six UN official languages.

[338] As a basis for this, the CBM refers to the following section from previous reports: UN General Assembly (2021): Developments in the field of information and telecommunications in the context of international security. (A/AC.290/2021/CRP.2). (Paragraph 50). & UN General Assembly (2022): Developments in the field of information and telecommunications in the context of international security. (A/77/275). (first APR, Recommended Next Steps, paragraph 5).

[339] UN General Assembly (2024): Paper by the Secretariat. Mapping exercise to survey the landscape of capacity-building programmes and initiatives within and outside the United Nations and at the global and regional level.

CBM's implementation.[340] Such examples illustrate that, even without formalized requirements, the CBM is already being **widely implemented** implicitly.

Member states have also recognised that many states require capacity-building support to develop national policies, strategies, and laws that underpin a secure ICT environment. In response, initiatives, such as UNIDIR's annual Cyber Stability Conference, workshops, and training programmes facilitated by the ITU and other organisations, have been highlighted as key enablers.[341] These efforts reinforce the linkages between this CBM and CBMs 5 and 6.

CBM 4

CBM 4 (2023): *"Encourage opportunities for the cooperative development and exercise of CBMs."*

Background: First articulated in the second APR (2023), this CBM builds on earlier reports and emphasises the importance of cooperation in CBM implementation at the bilateral, regional, and multilateral levels.[342] Regional organisations play a particularly important role, as many already operate cyber CBMs tailored to their specific contexts. The measure also stresses that the global list of CBMs is not exhaustive, and that existing CBMs must be implemented cooperatively rather than remain only on paper.[343]

Practice: This CBM is broad in scope, recognising that CBM implementation must account for diverse national and regional circumstances and can extend beyond measures formally defined by the UN. In this context, the exchange of views within the OEWG on the development and application of CBMs directly fulfills this measure under the UN framework.[344] It should be noted that cross-regional

[340] Australia as part of the OEWG Confidence Builders (2023):Joint Working Paper. Cyber CBMs in Action.

[341] UN General Assembly (2024): Paper by the Secretariat. Mapping exercise to survey the landscape of capacity-building programmes and initiatives within and outside the United Nations and at the global and regional level.

[342] As a basis for this, the CBM refers to the following section from previous reports: UN General Assembly (2023): Developments in the field of information and telecommunications in the context of international security. (A/78/265). (second APR, paragraph 53).

[343] As a basis for this, the CBM refers to the following section from previous reports: UN General Assembly (2023): Developments in the field of information and telecommunications in the context of international security. (A/78/265). (second APR, CBM section, Recommended Next Steps, paragraph 1).

[344] As a basis for this, the CBM refers to the following section from previous reports: UN General Assembly (2023): Developments in the field of information and telecommunications in the context of international security. (A/78/265). (second APR, CBM section, Recommended Next Steps, paragraph 1).

dialogue also occurs within the OEWG, since representatives from OAS and OSCE – who specialise in cyber issues – participate in these discussions.

CBM 4 also acknowledges the possibility of developing new measures. This has already materialised: four additional CBMs were articulated in the third APR (2024) and later endorsed in the OEWG's final report. These can be seen as an outcome of this CBM, even though their explicit practical implementation is still pending. Thus, this CBM can be considered **widely implemented**, though difficult to quantify, as there is no agreed upon vision of what full implementation should look like. The Confidence Builders have further emphasised the links between this CBM and OAS CBM 4 and OSCE CBM 5.[345]

CBM 5

CBM 5 (2024): *"Promote information exchange on cooperation and partnership between States to strengthen capacity in ICT security and to enable active CBM implementation."*

Background: First articulated in the third APR (2024), this CBM highlights the importance of capacity-building programmes as an "important avenue of collaboration which could strengthen relationships as well as build trust and enhance confidence between States."[346] Capacity is recognised as essential for CBM implementation.[347] For example, states need a national cybersecurity strategy to contribute to transparency (CBM 3), or functioning governance structures to nominate PoCs (CBM 1).[348] Cooperation in capacity-building is also confidence-building in itself, as such programmes often involve the disclosure of weaknesses and sensitive information. Increased trust, in turn, improves cooperation and reduces duplication in these efforts.

Practice: No explicit implementation measures have yet been taken for this CBM. However, many related initiatives exist, making CBM 5 **widely implemented** implicitly: the OEWG has served as a platform for states to exchange information on capacity-building needs, initiatives, and partnerships. Each session has included

[345] OEWG Confidence Builders (2023): Joint Working Paper. Building Confidence and Capacity in a Cyber Way, Confidence Builder.

[346] UN General Assembly (2024): Developments in the field of information and telecommunications in the context of international security (A/79/214).

[347] UN General Assembly (2024): Paper by the Secretariat. Mapping exercise to survey the landscape of capacity-building programmes and initiatives within and outside the United Nations and at the global and regional level.

[348] Pawlak, Patryk (2016): Confidence-Building Measures in Cyberspace: Current Debates and Trends. In: Osula, Anna-Maria and Rõigas, Henry (Eds.): International cyber norms. Legal, policy & industry perspectives. NATO Cooperative Cyber Defence Centre of Excellence.

a dedicated discussion on capacity-building, contributing to greater transparency in this area and underlining once again that the OEWG itself functions as a CBM. The UNIDIR Cyber Policy Portal also supports this CBM, in connection with the Cybil Portal (launched in 2019 by the Global Forum on Cyber Expertise). Cybil serves as a central repository for international cyber capacity-building projects[349] and currently contains around 1,000 projects. In 2023, the UN Secretariat was tasked with mapping global and regional capacity-building initiatives, drawing on member state input.[350] The resulting 2024 report provides a global overview and implicitly supports this CBM.

Furthermore, the OEWG's final report proposes creating a Global ICT Security Cooperation and Capacity-Building Portal (GSCCP), which could provide additional support for CBM implementation if issues of sustainable funding and duplication with existing platforms are resolved.[351] States have also suggested practical tools, such as Kazakhstan's proposal for a CCB template to streamline requests and match needs with offers.[352] This CBM is also connected to CBM 1, as the directory "could serve as platforms for capacity-building" and the PoC Directory could be linked to the GSCCP.[353] It is important to note that these initiatives developed independently of this CBM and collectively contribute to its implicit implementation.

CBM 6

CBM 6 (2024): *"Engage in regular organization of seminars, workshops and training programmes on ICT security."*

Background: Introduced in the third APR (2024), this CBM seeks to promote communication and mutual understanding by encouraging the regular organisation of seminars, workshops, and training programmes on ICT security issues.[354]

[349] UN General Assembly (2024): Paper by the Secretariat. Mapping exercise to survey the landscape of capacity-building programmes and initiatives within and outside the United Nations and at the global and regional level.

[350] UN General Assembly (2023): Developments in the field of information and telecommunications in the context of international security. (A/78/265).

[351] UN General Assembly (2025): Draft Final Report (A/AC.292/2025/CRP.1). // See a report on more suggestions in this regard here.

[352] Kazakhstan's Representative (2025): (5th Meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (3-7 March 2025).

[353] UNODA (2024): Initial background paper on capacities required to participate in a global intergovernmental points of contact directory.

[354] UN General Assembly (2024): Developments in the field of information and telecommunications in the context of international security (A/79/214).

Practice: Such workshops, training programmes, and seminars are a typical capacity-building activity. Thus, CBM 6 is connected to CBM 5. As with CBM 5, CBM 6 has not yet been explicitly implemented, but it builds on countless bilateral, regional, and multilateral training activities, as well as side-events on the margins of the OEWG meetings, resulting in this CBM being **widely implemented** in an implicit manner. Activities by UNIDIR contribute to implicitly implementing this CBM by regularly facilitating trainings and events. A specific example is its "training on norms, international law and cyberspace" course, which deepens understanding of this framework and assists member states, for instance, in the development of national positions on how international law applies in the cyber domain, thereby contributing to building capacities and confidence.[355]

The OEWG has also served as a venue for information exchange on such efforts, particularly under its capacity-building agenda item. The above-mentioned possible establishment of a dedicated GSCCP could further enhance coordination of these efforts and thus implicitly contribute to this CBM's implementation since it is proposed that this portal could be "a central location for providing practical information on ICT security events to foster the active participation of States."[356] CBM 6 also connects to CBM 1, since states have acknowledged that "[c]apacity-building activities such as training sessions, seminars and other initiatives were noted as useful for strengthening expertise, knowledge and cooperation, which would in turn allow for more effective engagement in the directory."[357]

CBM 7

CBM 7 (2024): *"Exchange information and best practice on, inter alia, the protection of critical infrastructure (CI) and critical information infrastructure (CII), including through related capacity-building."*

Background: First articulated in the third APR (2024), this CBM focuses on strengthening state resilience in protecting CI and CII. It highlights the cross-cutting role of capacity-building (linking it to CBM 5) and recognises a strong connection with CBM 8, since much critical infrastructure is operated by private actors.

[355] See here.

[356] UN General Assembly (2025): Draft Final Report (A/AC.292/2025/CRP.1).

[357] UNODA (2024): Initial background paper on capacities required to participate in a global intergovernmental points of contact directory.

Practice: To date, **no implementation**, or at least no concrete steps have been taken to explicitly implement this CBM. However, states have used the OEWG to exchange information and practices related to CI and CII protection, which implicitly contributes to this CBM's implementation since it is to be implemented primarily through the exchange of information.[358] The OEWG's 2025 final report specifically proposes "further study of concrete measures on how CBMs can be used in the case of severe ICT incidents affecting CI and CII."[359]

CBM 8

CBM 8 (2024): *"Strengthen public-private sector partnerships and cooperation on ICT security."*

Background: This CBM was also first articulated in its current form in the third APR in 2024 and acknowledges that "[a] range of technical capabilities and knowledge are required to detect, defend against and respond to and recover from ICT incidents."[360] Much of the digital infrastructure is privately owned, and private companies are frequently the primary targets of cyber operations,[361] thus, it is crucial to build PPPs to effectively address ICT security.

Practice: The OEWG has served as a platform for states to share information on national efforts and good practices, which contributes implicitly to this CBM since it is to be implemented primarily through the exchange of good practices. In addition, the measure anticipates regular public–private dialogue. While private sector participation in the OEWG was limited – restricted to accredited representatives who had only brief opportunities to contribute – their presence nonetheless supported this CBM's partial implementation.[362] This is also supposed to be the case in the future Global Mechanism.[363] Several member states, led by Chile and Canada, have actively promoted greater stakeholder involvement within the OEWG, by organising events to engage non-state stakeholders and via working papers, for instance, by proposing practical modalities of what stakeholder participation could look like in the future permanent mechanism as well as by

[358] UN General Assembly (2024): Developments in the field of information and telecommunications in the context of international security (A/79/214).

[359] UN General Assembly (2025): Draft Final Report (A/AC.292/2025/CRP.1).

[360] UN General Assembly (2024): Developments in the field of information and telecommunications in the context of international security (A/79/214).

[361] Ciglic, Kaja, and Hernig, John (2021): A multi-stakeholder foundation for peace in cyberspace. Journal of Cyber Policy 6 (3), p. 360-274.

[362] UN General Assembly (2024): Developments in the field of information and telecommunications in the context of international security (A/79/214).

[363] UN General Assembly (2025): Draft Final Report (A/AC.292/2025/CRP.1).

setting out best practices that reflect contributions from industry, civil society, the technical community, and academia. Thus, this CBM is **implemented, but not widely**.

4.4.3. Implementation on the global level builds on long-standing (regional) efforts

The UN's universality is both a strength and a challenge when it comes to cyber CBM implementation. It brings together states with vastly different levels of cyber maturity, experience with CBMs, geopolitical interests, and policy priorities. These disparities often complicate consensus and slow progress. In contrast, regional forums can foster tailored, confidence-building initiatives more easily. Yet not all states belong to such organisations, and not all regional organisations have cyber CBMs in place – reinforcing the continued importance of maintaining cyber CBMs at the global level. The OEWG has repeatedly highlighted the value of regional efforts, framing them as complementary to UN-level initiatives.

The formulation and implementation of cyber CBMs at the UN level has been a long and gradual process. States proposed the nomination of national PoCs as early as the 2013 GGE report. Yet, the global directory only went live in 2024, and further work remains to make it fully operational. Of the eight agreed on cyber CBMs, only CBM 1 has seen substantial explicit implementation. However, several others have been advanced through implicit activities that contribute to achieving their objectives, even if these efforts are not formally labelled or reported as implementation measures. CBM 1 has drawn the most attention in recent years due to its foundational role in the implementation of further cyber CBMs.

The broad and sometimes vague formulation of the cyber CBMs – only the last two being more topic-specific – has had mixed effects. On the one hand, most build on long-standing (regional) efforts and previously recommended measures, which helped secure consensus and allowed existing UN tools and platforms to be used. On the other hand, their breadth makes systematic assessment of implementation difficult. CBM 1 is the only measure with a clearly verifiable delivery. Moreover, the CBMs are inherently interconnected. For example, the PoC Directory (CBM 1) could be used to share information on cooperation and partnerships (CBM 5) or to circulate updates on workshops (CBM 6) that, in turn, are central to exchanging best practices on CI protection (CBM 7), where PPPs (CBM 8) are especially valuable. This overlap is not necessarily a weakness, as it can foster efficiency and political will. However, it does blur the boundaries between measures, complicating assessments of what implementation actually entails. Sustained awareness-raising will remain essential given the uneven levels of CBM experience among states.

One consistent takeaway is that the OEWG itself functions as a CBM and plays a crucial role when it comes to the implementation of cyber CBMs. It has enabled cross-regional dialogue, fostered trust, and created a forum for transparent exchange. This role will likely continue under the future permanent mechanism. Coordination between global and regional cyber CBM efforts is also improving. For example, the UN, OSCE, and OAS secretariats are collaborating on their PoC directories, while ECOWAS has encouraged its PoCs to serve simultaneously as UN PoCs.[364]

A promising trend has also emerged in recent OEWG sessions: more states now highlight their national cyber CBM activities and explicitly link them to specific cyber CBMs.[365] Such efforts help clarify the purpose of each measure, bring them to life, and provide models for others to follow. Moreover, this trend is crucial because the secretariat UNODA has no mandate to track cyber CBM implementation and relies on state reporting. At the same time, these examples – ranging from highlighting conferences and novel laws, joint research projects, or capacity-building efforts – also show how broad the idea of implementing these CBMs is since they are formulated in a very broad manner. It further underlines in its implementation the cyber CBMs' implicit nature and interconnectedness.

The open, informal, cross-regional Confidence Builder group of states[366] has also made an important contribution to raising awareness and developing a shared vision of how cyber CBMs can be implemented. Additionally, the UNIDIR survey also includes questions on cyber CBM implementation, and could provide a useful starting point for more structured and transparent reporting.

[364] ECOWAS as part of an open, informal, cross-regional Group (2025): Non-Paper. Inter-regional Cooperation - The Role of Regional Organizations in Implementing the UN Framework for Responsible State Behaviour in Cyberspace.

[365] e.g. Germany (2024): "I would like to focus in particular on CBM2 (...) and CBM6 (...). As part of our ongoing CBM implementation efforts and in line with our G7 ECOWAS cybersecurity action plan, Germany organized a study trip of an ECOWAS delegation to Vienna in September this year. The delegation, alongside representatives from the OAS, the African Union, and the OSCE, participated in the inter-regional conference on cybersecurity organized by the Republic of Korea, North Macedonia, and the OSCE Secretariat. Moreover, the ECOWAS delegation observed a meeting of the informal working group of the OSCE, which provided useful insights into regional CBM implementation practices." (Germany's representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Ninth Substantive Session (2-6 December 2024)) or UK (2024): "In support of CBM 7, the UK continues to develop and share tools to raise the resilience of critical national infrastructure internationally. Since 2019, the UK has supported the assessment of national cybersecurity risks in nearly 20 countries" (UK's representative (2024): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Ninth Substantive Session (2-6 December 2024)).

[366] The following OEWG participating states are members of this group: Australia, Brazil, Canada, Chile, Colombia, Czech Republic, Dominican Republic, Fiji, Ghana, Germany, Israel, Jordan, Republic of Korea, Mexico, The Netherlands, Singapore, Uruguay.

Despite these challenges, the adoption of the eight UN cyber CBMs is widely regarded as one of the OEWG's most concrete achievements, especially in light of geopolitical tensions that have stalled progress in other areas.[367] Cyber CBMs have provided a rare platform for constructive engagement. Still, political friction is never far away. At the ninth OEWG session in 2024, for example, France raised concerns about possible misuse of the PoC directory – concerns later echoed in a joint statement with Germany.[368]

Throughout the process, states have also advanced new proposals, including Iran's controversially received[369] suggestion for a cyber CBM on ensuring unhindered access to secure ICT markets,[370] and recommendations in the APRs to promote transparency by encouraging states to share their interpretations of key technical ICT terms. The OEWG's final report leaves the door open for further cyber CBM development under the future permanent mechanism. However, most member states agree that the immediate priority should be the implementation of the existing eight CBMs.[371] The challenge now is to implement them, "to put meat on the bone," by identifying practical steps, including mechanisms for dialogue and monitoring.[372] Sustained efforts will also be required to identify and overcome barriers to implementation and to connect these with capacity-building opportunities.[373]

[367] Radunović, Vladimir, Kazakova, Anastasiya, Ittelson, Pavlina, Petit Siemens, Salomé, Gavrilović, Andrijana (2025): UN OEWG concludes, paving way for permanent cybersecurity mechanism.

[368] France's Representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Ninth Substantive Session (2-6 December 2024): "(…) France, at the same time, wishes to reiterate its call to not exploit this tool, to not overuse the tool, at the risk of making it inoperable (…)" // Germany's Representative (2025): (6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Tenth Substantive Session (17-21 February 2025) in a joint statement with France: "(…) It is not sensible to continue sending identical requests when a clear avenue to seek remedies to an alleged malicious cyber activity has been provided on numerous occasions. Such actions seem to be aiming at spamming our cybersecurity agencies, which are committed to responding to such queries in good faith. Such practices bear the risk to undermine, in the eye of the practitioners, the credibility of our diplomatic work here at the UN. And this contradicts the purpose of the future mechanism to bridge the gap between the technical and the diplomatic communities. Taken together, in our view, such activities undercut the meaningful objective of the global POC directory (…)."

[369] Iran's proposal was backed by Brazil and El Salvador for example, however, Western states like Canada, United States, Ukraine, the EU, and Australia opposed adding a new CBM, maintaining their position that the focus must now be on implementing the existing CBMs. Switzerland suggested moving the proposal to the CCB section, where voluntary ICT assistance could be offered. The overall critique regarding this CBM proposal is that it would benefit states seeking to circumvent Western sanctions, including Iran, Russia, and China, since the emphasis on universal technology access would make it harder to argue against granting certain states such access (see here and here).

[370] see the proposal here.

[371] UN General Assembly (2025): Draft Final Report (A/AC.292/2025/CRP.1). // Several statements of states at the eleventh substantial session of the OEWG, find the transcripts here.

[372] UN General Assembly (2025): Draft Final Report (A/AC.292/2025/CRP.1)

[373] OEWG Confidence Builders (2022): Working-Paper to advance the ongoing Discussions within the United Nations Open Ended Working Group (OEWG) on Confidence Building Measures (CBM) in Cyberspace.

4.5. Economic Community of West African States (ECOWAS)

4.5.1. Formulation of ECOWAS cyber CBMs

Founded in 1975, the Economic Community of West African States (ECOWAS) was established to strengthen economic and political integration across West Africa. Today, it counts 12 member states[374] and promotes regional cooperation, collective self-sufficiency, and sustainable development across diverse areas, including trade, infrastructure, governance, and security. Its mandate also extends to conflict prevention, peacekeeping, and addressing transnational challenges that threaten regional stability.

In recent years, ECOWAS has increasingly recognised the central role of digital infrastructure in both economic growth and security. Cybersecurity has accordingly become a regional priority, with efforts directed at raising awareness among member states, supporting capacity-building initiatives in cooperation with international partners, and fostering collaboration in combating cybercrime. By the end of 2024, ECOWAS had formally adopted three cyber CBMs.[375]

These cyber CBMs emerged through a collaborative process involving the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and the Global Forum for Cyber Expertise (GFCE) under the Joint Platform for the Advancement of Cybersecurity in West Africa. Over the course of two years, a series of workshops, including tabletop exercises and a study visit to the OSCE IWG meeting, facilitated the joint development and formulation of cyber CBMs. While numerous cyber CBMs were proposed throughout this process, a consensus was ultimately reached on three key measures.[376]

As part of this process, ECOWAS member states also agreed to establish an informal, open-ended working group of national cybersecurity experts supported by the ECOWAS Commission. Since 2025, the group has convened at least annually to review progress on cyber CBM implementation and exchange views and information on cybersecurity developments.

[374] Benin, Cabo Verde, Côte d'Ivoire, The Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Nigeria, Sénégal, Sierra Leone, and Togo. It was founded by 15 member states, Burkina Faso, Mali and Niger withdrew from ECOWAS in January 2025 due to deteriorating relations between the states and the rest of the ECOWAS region. See more here.

[375] ECOWAS (2024): Directive C/DIR.2/12/12 on Cyber/ICT Confidence Building Measures.

[376] Ghana's Representative (2024): (7th meeting) Open-ended working group on Information and Communication Technology (ICT) - Ninth Substantive Session (2-6 December 2024).

4.5.2. Implementation of ECOWAS cyber CBMs

CBM 1

CBM 1 (2024): *"Share information on Cybersecurity related documentation"*

Background: CBM 1 is designed to foster transparency and predictability among member states by encouraging the exchange of national cybersecurity policies, strategies, regulations, best practices, threat assessments, and programmes. This openness provides insight into national priorities, strategic objectives, and governance structures. It also notes that where relevant, member states may highlight how their approaches align with regional practices, helping identify common ground and potential areas for cooperation. This openness fosters mutual trust and understanding, enabling partners to better anticipate each other's actions and policies in the cyber domain and reduce the risk of misperceptions.

Practice: There is **no implementation** activity as of yet. The next step is to establish a web portal through which the documents can be shared accordingly. It is currently being examined whether existing portals, such as the ECOWAS Cyberportal, which was established in 2019 through a partnership with France and the EU via the OCWAR-C project aimed to fighting cybercrime,[377] can be used for this purpose.

CBM 2

CBM 2 (2024): *"Designate National points of contact"*

Background: CBM 2 seeks to strengthen regional cyber stability by designating national PoCs at both the diplomatic and technical levels. These PoCs serve as reliable channels for timely communication in the event of cyber incidents, allowing states to clarify intent, share information, and reduce the risk of escalation. By facilitating coordinated dialogue on cybersecurity at the national, regional, and international levels, the measure fosters trust and cooperation while ensuring that every member state has an established, dependable link for both diplomatic and technical engagement on cyber issues.

Practice: All member states have recently nominated their PoCs and the ECOWAS Commission is tasked with managing the PoC network. The next step is to establish a web portal through which the PoC Directory can be used accordingly

[377] Find more on it here.

(linked to CBM 1). A distinctive feature of this CBM is the encouragement of states to nominate the same PoCs they use for the UN's Global PoC Directory (UN CBM 1), thereby promoting consistency, strengthening cross-regional cooperation, and building on existing structures. This explicit reference is due to the fact that the Global PoC Directory already existed at the time this CBM was formulated. In addition to nominating PoCs, coordination between the technical and diplomatic PoCs at the national level should ideally take place; this is supposed to be enhanced now within each state. Moreover, an aim is to establish procedures for regularly updating contact information through ping tests, which are planned to be carried out for the first time in late 2025.

Although implementation is still in its infancy, it has met with widespread approval. This CBM is already **widely implemented**, with all member states having swiftly nominated their PoCs. It remains to be seen to what extent the directory will actually be used and updated in the future.

CBM 3

CBM 3 (2024): *"Raising awareness on cyber threats and remediation measures"*

Background: This CBM responds to a persistent regional challenge: uneven levels of cyber awareness and preparedness among states that create vulnerabilities that can be exploited by malicious actors. Because one state's weaknesses can compromise the entire region, raising awareness and building capacity is critical.[378] Activities may target a range of stakeholders, including government institutions, technical experts, and the general public. CBM 3 aims to strengthen collective resilience by closing knowledge gaps and promoting regular exchanges.

Practice: Implementation could take many forms. Public-facing initiatives might include social media campaigns, radio or television broadcasts, or printed awareness materials, while more specialised efforts could involve workshops, conferences, and expert roundtables. Such activities would ensure that information reaches both the technical communities and wider public. Member states are also expected to use expert group discussions to exchange views on CBM implementation and to consider introducing additional measures in the future. This CBM builds on earlier joint or domestic efforts, for example, activities like "Ghana's Cyber Security Awareness Month."[379] However, **no implementation** has taken place so far within the context of explicitly implementing this CBM.

[378] KnowBe4 Africa & Red Ribbon Insights (2025): KnowBe4 Africa Human Risk Management Report 2025: The Human Element in African Cybersecurity Insights From Decision-Makers.

[379] Find more on it here.

4.5.3. Implementation still pending

As of 2025, the implementation of the three ECOWAS cyber CBMs remains in its early stages.[380] Initial progress includes the remarkably quick nomination of the PoCs and the first meeting of the regional expert working group. Additional concrete steps are planned such as establishing a web portal facilitating the implementation of CBMs 1 and 2 as well as ping tests supporting CBM 2.

It should be noted that the process from the initial idea to the adopted cyber CBMs was very quick, certainly because the first two CBMs are already proven cyber CBMs and the third answers a specific regional need and builds on earlier efforts that have already gone on for years at the national level as well. Another relevant aspect and distinctive regional feature is the initial involvement of international partners. In this context, logistical and financial support were provided and experiences were exchanged, for example, through the OSCE study trip, which also took place in the context of OSCE CBM 12's implementation.

ECOWAS' cyber CBMs are embedded in the socio-economic context, meaning that they are intended to contribute to minimising economic losses caused by cyber incidents. It remains to be seen how deeply these cyber CBMs will take root in practice and whether additional measures will be introduced - something that is definitely planned. Importantly, CBM 3 explicitly leaves the door open for further development.

ECOWAS has positioned itself as the first African region to equip its cyber diplomats and experts with a dedicated set of cyber CBMs – a significant step toward strengthening regional cyber resilience. It is also noteworthy that these cyber CBMs are the first formalised CBMs within ECOWAS – unlike most other regional organisations, which already have formalised CBMs in other areas within the organisation's common context. Another crucial regional characteristic is that, although CBMs are generally voluntary, these cyber CBMs within the ECOWAS framework were decided upon by a directive. In other words, the goal is legally defined. However, it is up to the member states to decide how to achieve it, so the implementation details are not specified.

[380] ECOWAS as part of an open, informal, cross-regional Group (2025): Non-Paper on Inter-regional Cooperation. The Role of Regional Organizations in Implementing the UN Framework for Responsible State Behaviour in Cyberspace.

4.6. Conference on Interaction and Confidence Building Measures in Asia (CICA)

The Conference on Interaction and Confidence Building Measures in Asia (CICA) was established in 1992 as a multilateral forum to enhance cooperation and promote peace, security, and stability across Asia. Today, it brings together 28 member and 10 observer states,[381] serving as a platform for dialogue on a broad spectrum of political, security, economic, environmental, and humanitarian issues. Its CBMs span these areas.[382]

Recognising the growing importance of cybersecurity for regional stability, CICA updated its Catalogue of Confidence Building Measures in 2021 to add a new priority area on the "Security of and in the Use of Information and Communication Technologies (ICTs)." The following five CBMs were adopted:[383]

- **CBM 1 (2021):** *"Promoting an open, secure, peaceful, and cooperative ICT environment in Asia on the basis of mutual respect, strengthening of contacts and exchanges, deepening of dialogue and cooperation, fighting against threats resulting from the malicious use of ICTs."*
- **CBM 2 (2021):** *"Promoting dialogue on confidence-building, stability and risk reduction in the field of security of and in the use of ICTs among CICA member states."*
- **CBM 3 (2021):** *"Recognising the importance of peaceful use of ICTs by reducing misunderstanding between CICA member states, promoting trust and confidence."*
- **CBM 4 (2021):** *"Sharing information, best practices and raising awareness in the field of security of and in the use of ICTs to address the threats stemming from the use of ICTs."*
- **CBM 5 (2021):** *"Improving cooperation to respond to the criminal use of ICTs based on an internationally agreed legal framework."*

These CBMs are broadly formulated and, to a large extent, primarily emphasise a shared vision and commitments. Explicit steps for implementation are difficult to discern from the wording as they are not operationally oriented, for example, to deal with ICT incidents, but are aimed in particular at mutual information exchange, for

[381] Afghanistan, Azerbaijan, Bahrain, Bangladesh, Cambodia, China, Egypt, India, Iran, Iraq, Israel, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Mongolia, Pakistan, Palestine, Qatar, Republic of Korea, Russia, Sri Lanka, Tajikistan, Thailand, Turkiye, UAE, Uzbekistan, and Viet Nam; observer states: Belarus, Indonesia, Japan, Laos, Malaysia, Philippines, Saudi Arabia, Turkmenistan, Ukraine, United States.

[382] Find the catalogue of Confidence Building Measures as amended in 2024 here.

[383] Find them here.

example through the exchange of best practices, strengthening contacts and exchange between them, and deepening dialogue and cooperation. Emphasis is also placed on awareness raising and cooperation to respond to the criminal use of ICTs.

The main drivers behind this process have been China and Russia, which initiated work in this thematic area and have served as co-coordinators since 2022, with their mandate extended until 2025.[384] They have largely overseen the implementation of activities, which has so far taken the form of workshops. Since 2022, these workshops have addressed topics such as the sustainable and secure development of the internet, sharing experiences on countering the criminal use of ICTs, digital forensics, and raising awareness of ICT security to address emerging threats.[385] While these activities reflect incremental progress, implementation has remained limited and is low-visibility. CICA rarely appears in UN discussions or international research on cybersecurity, underscoring its relatively modest profile in this field.

CICA's member states form a highly diverse group, differing in culture, security priorities, and levels of cyber maturity. Despite these differences, the forum has articulated a clear long-term vision: to transform into a full-fledged regional organisation through the inclusive, consensus-based process launched by the 2022 Astana Statement.[386] The transformation roadmap aims to reinforce institutional foundations by adopting a charter, reforming budget and human resources, updating procedures, and strengthening the role of the Secretariat to deepen cooperation.[387] While CICA is not yet on par with institutionalised regional organisations, it is included here for completeness, as it is one of the few frameworks to have adopted explicitly formulated multilateral cyber CBMs.

[384] CICA (2024): Concept paper and plan of implementation of the CICA confidence-building measure "Security of and in the use of ICTs" for 2024-2025.

[385] Find examples here and here.

[386] See here.

[387] See here.

5. Putting words into practice: Key takeaways

The state of implementation of cyber CBMs demonstrates that regions across the world increasingly view cyber CBMs as a valuable diplomatic tool for enhancing security and stability in the cyber domain. Many have committed to their adoption and implementation in recent years, and more continue to join this trend – either by formally endorsing cyber CBMs or actively negotiating their introduction. This highlights the crucial role of regional organisations in adapting global agreements to regional realities and serving as a bridge between global and regional levels.

At the same time, implementation remains a work in progress. While numerous initiatives are underway, the degree of progress varies: some measures are being actively implemented, others are still at an early stage, and much remains to be done. Importantly, even for cyber CBMs that are already well established, there is room for more ambitious interpretation and further practical action to deepen their impact.

Measuring implementation is challenging. Unlike arms control treaties, CBMs are voluntary, flexible, and (mostly) not designed for verification. They do not prescribe a rigid work plan, and their success cannot be precisely quantified. For instance, it is impossible to calculate how many cyber operations were deterred or de-escalated because cyber CBMs were in place. Even so, it is possible to identify areas where substantial implementation has occurred either in an explicit or an implicit manner, based on observable state practice rather than impact. Based on the analysis, several key findings emerge:

- **Formulation is easier than implementation:** From the outset, the drafting process (step 1: formulation) emphasised finding language that could secure consensus among states, leaving implementation details to later. In other words: formulating cyber CBMs is the easier part, sustaining implementation is much harder.
- **Explicit deliverables facilitate measurability:** Some CBMs are formulated in a way that they have clear deliverables, such as nominating PoCs. The implementation of such cyber CBMs is easier to monitor, with progress often published by regional secretariats. In contrast, information on other cyber CBMs is not publicly known, or it is more difficult to identify, especially if the implementation is mostly implicit. In fact the state of implementation shows, many implicitly implemented cyber CBMs depend on prior national-level efforts, such as developing strategies or technical tools.

- **Dialogue is a core outcome:** Some cyber CBM reaffirm existing commitments rather than introduce new ones (e.g., OAS CBM 9). In practice, the process of sharing experiences and best practices is thus often as valuable as the end product. Dialogue itself fosters trust and confidence, even where fixed deliverables (like an incident severity scale or a position on international law in cyberspace) are absent or developed due to domestic priorities. In addition, the actual deliverable of many cyber CBMs is, of course, dialogue (e.g., UN CBM 2).
- **CBMs often work best as interconnected systems:** A lot of cyber CBMs function best as interconnected systems rather than isolated measures. For example, within the OSCE, mechanisms such as consultation (CBM 3), crisis communication (CBM 10 and 13), and PoCs (CBM 8) work in tandem. Alone, each would have limited utility; together, they form a coherent framework. Similarly, establishing a working group may serve as a means to sustain engagement while laying the groundwork for more substantive cooperation.
- **Capacity-building is foundational:** A lot of cyber CBM activities either aim to build up capacities or are connected to capacity-building measures as capacity itself is a prerequisite for successful implementation.
- **Success should not solely be measured via explicit outputs:** Cyber CBMs are often portrayed as low-hanging fruit for negotiators seeking to achieve outcomes, given that they are non-binding and are usually not verified. In practice, however, their implementation is far from simple. Building the necessary trust and willingness to share information – particularly on sensitive cyber matters – remains a slow and complex process. Yet cyber CBMs play an important role in sustaining dialogue and enabling initial steps toward cooperation when political space for deeper engagement is limited. Thus, the success of cyber CBMs should not be measured in isolation based on the explicit activities to implement individual cyber CBMs, but should also consider the broader framework of communication and trust they create. Especially in times of geopolitical tension, the ability of cyber CBMs to maintain communication channels may matter more than achieving explicit implementation breakthroughs. This was highlighted for instance by Germany reporting that it chose to increase its engagement in the OSCE cyber CBMs due to "heightened geopolitical tensions in the OSCE area"[388] by sharing information on major cyber incidents more actively through the PoC Network since May 2022.
- **Implementation is a continuous process:** Implementation is not a one-off exercise but a continuous, long-term commitment. Even "widely implemented" CBMs – like the OSCE's CBM 11 – require sustained engagement to remain relevant and functional.

[388] Germany as part of the OEWG Confidence Builders (2023): Input Paper, CBMs in Action.

- **There is no universal model for implementation:** The OSCE, OAS, and ECOWAS each have secretariats with mandates and resources to support implementation, whereas the ARF operates without a specifically dedicated body, relying instead on co-sponsoring states to drive activities. The OSCE's adopt-a-CBM-initiative represents yet another approach aimed at fostering ownership. ARF implementation is largely workshop-based, while other organisations employ a wider set of instruments depending on the specific cyber CBM.
- **Regional variation reflects diverse contexts:** These differences are not limited to how organisations implement cyber CBMs but also extend to what they prioritise: the OAS emphasises capacity-building and the translation of global commitments into regional practice; the OSCE has developed crisis communication mechanisms and aims to expand engagement with the private sector; and ECOWAS has prioritised awareness-raising as a foundational step.
- **Cross-regional exchange is crucial:** The organisations draw on each other's experiences and maintain cross-regional exchanges – for instance, within the UN OEWG and other, more informal settings. Certain CBMs – such as the establishment of PoC directories and the sharing of national strategies, echoing traditional Cold War precedents – have become foundational across all multilateral organisations, and initial discussions are emerging on linking these initiatives. Indeed, these measures are among the most widely implemented within each organisation.

Moving forward, clarifying and communicating more broadly what successful implementation of individual cyber CBMs entails, the possible pathways to achieve it, and how current progress compares could help enhance visibility, facilitate learning, and guide future implementation efforts. Greater cross-regional exchange and tailored capacity-building could support the necessary sustainable, long-term implementation of CBMs in the cyber domain. Further research could focus on identifying key enablers and obstacles to implementation – such as institutional design, political incentives, and resource allocation. Finally, examining the interplay between formal cyber CBMs and informal trust-building mechanisms – including technical exchanges and expert networks – may reveal new pathways for deepening cyber stability and cooperation.

Annex

I. Examples of different cyber operations

Examples of false flag operations

In 2016, Russian military intelligence units (26165 and 74455) compromised the networks of the Democratic National Committee (DNC) and Democratic Congressional Campaign Committee (DCCC) through spearphishing, copying emails and sensitive documents. To conceal their involvement and mislead attribution, they launched DCLeaks.com and claimed to be American Hacktivists. Later on, they created the **Guccifer 2.0** persona, falsely claiming to be a lone Romanian perpetrator.[389] The operatives used VPNs, foreign servers, and embedded Cyrillic metadata to bolster the deception.[390] Despite these efforts, United States intelligence agencies at some point confirmed the GRU was behind the operation interfering in the United States presidential election.[391]

The **Sony Pictures compromise** in 2014 was a degradating cyber operation by a group calling itself the Guardians of Peace, which leaked sensitive data and crippled Sony's systems. Initially, the perpetrators issued a ransom demand, a move more typical of criminal groups than state actors, which misled investigators. Combined with the use of common malware and third-country infrastructure (using the high-speed network of a hotel in Bangkok), this tactic delayed attribution.[392] The United States eventually attributed the operation to North Korea's Lazarus Group (APT38), framing it as retaliation for the movie "The Interview", though Pyongyang denied any involvement.[393]

[389] Read more on the Guccifer 2.0 Persona here and find his Blog here.

[390] CrowdStrike (2020): CrowdStrike's work with the Democratic National Committee: Setting the record straight.

[391] US Department of Justice (2018): Press Release: Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election.

[392] TrendMicro (2014): The Hack of Sony Pictures: What We Know and What You Need to Know.

[393] FBI (2014): Update on Sony Investigation.

Examples of operations causing damage beyond the target

Stuxnet, discovered in 2010, targeted Iran's Natanz uranium enrichment facility, sabotaging centrifuge operation by exploiting four zero-day vulnerabilities in Siemens' underlying Windows operating system. Infection happened via USB flash drives or open network shares, afterwards the infected system could be controlled by the perpetrator giving them full control,[394] even including a command and control function via two servers.[395] However, once released, the malware spread beyond its intended target, infecting hundreds of thousands of systems worldwide. While it caused no direct damage to most of these machines, the incident led to enormous costs in detection and response efforts.[396] Experts widely attributed it to the US and Israel aiming to hinder the Iranian nuclear program.[397]

NotPetya (2017) was disguised as ransomware but functioned as a destructive wiper malware causing permanent data loss for those affected. NotPetya was deployed through a supply chain compromise in an Ukrainian tax software update (MeDoc) and exploited the "EternalBlue" vulnerability in Microsoft Windows, which was initially developed by the NSA.[398] Once in the system the malware spread autonomously. Though initially appearing as a financially motivated criminal operation, it was later attributed to Russian military intelligence GRU (Sandworm/APT44) as part of broader hybrid operations aiming to destroy Ukrainian targets.[399] However, the malware quickly spread beyond Ukraine, affecting 65 countries worldwide and around 49,000 systems from multinational corporations as well as the healthcare sector, with estimated damages exceeding 10 billion dollars.[400]

Supply chain compromises are another example of operations that can cause damage far beyond their intended target. By exploiting trusted software or hardware providers, perpetrators gain covert access to multiple

[394] Enisa (n.d.): Stuxnet Analysis.

[395] Falliere, Nicolas, O Murchu, Liam, Chien, Eric (2011): W32. Stuxnet Dossier.

[396] Gostev, Alexander (2010): Myrtus and Guava: the epidemic, the trends, the numbers.

[397] Risk and Resilience Team CSS, ETH Zürich (2017): Hotspot Analysis: Stuxnet.

[398] Hypr (n.d.): EternalBlue. Encyclopedia.

[399] United States Department of Justice (2020): Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace.

[400] Bendiek, Annegret and Schulze, Matthias (2021): Attribution: A Major Challenge for EU Cyber Sanctions. An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW. SWP Research Paper 11.

downstream victims across sectors and borders, often remaining undetected for long periods. These operations are difficult to remediate and can disproportionately affect neutral parties. While some may be limited to a single target, the interconnected nature of digital supply chains means such compromises can easily cascade into widespread disruption – either through large-scale exploitation by the original actor or opportunistic use by others – creating significant escalation risks.[401]

II. Examples of different kind of CBMs

Humanitarian CBMs typically precede formal negotiations and may include anti-personnel mine bans, prisoner exchanges (e.g., the 2011 Gilad Shalit exchange between Israel and Palestine[402]), or humanitarian ceasefires – such as those enabling aid delivery to Gaza in early 2025.[403] These measures often signal a mutual willingness to engage in dialogue to settle a conflict.

Political CBMs are designed to build trust between conflicting parties, particularly during negotiation phases. They can take simple forms such as informal meetings, shared spaces, or joint activities – for instance, during the 2002 Sudan North-South negotiations, football matches helped humanise the actors and facilitate dialogue.[404] In intra-state conflicts, political CBMs may include power-sharing, proportional representation, or institutional reforms to strengthen confidence in the state. After the 2001 conflict in North Macedonia, for example, CBMs involved phased police redeployment under international monitoring, recruitment of minority police cadets, and broader police reform – measures aimed at restoring trust between ethnic communities and the state, especially given the police's direct role in the conflict.[405]

Economic CBMs foster interdependence, making confrontation costlier and cooperation more attractive. In a globalised economy, such measures shape both interstate relations and interactions within states. Examples include opening trade routes, granting market or land access, or launching

[401] Lenaerts-Bergmans, Bart (2023): What is a Supply Chain Attack?

[402] See here.

[403] See here.

[404] Mason, Simon J. A. and Siegfried, Matthias (2013): Confidence Building Measures (CBMs) in Peace Processes. In: Managing Peace Processes. Process related questions. A handbook for AU practitioners, pp. 57–77.

[405] OSCE (2012): OSCE Guide on Non-military Confidence-Building Measures (CBMs).

joint development projects. In 2016, for instance, Moldova and Transnistria agreed to restore Moldovan farmers' access to land across the administrative border – reviving a 2006 agreement and helping to de-escalate territorial tensions.[406]

Environmental CBMs address shared challenges such as wildfires, floods, earthquakes, or droughts, which often cross borders and can intensify existing disputes. Since 2011, the OSCE has supported cooperation between Kyrgyzstan and Tajikistan in the Fergana Valley through training and canal renovation, reducing water-related tensions in a region complicated by unresolved border issues.[407] Similarly, Belize and Guatemala agreed in 2003 to cooperate on natural disaster response as part of efforts to ease a territorial dispute and prevent small-scale clashes.[408]

Societal and cultural CBMs focus on people-to-people engagement to reduce mistrust and foster mutual understanding in conflict-affected areas. Measures include releasing information on missing persons (e.g., Bosnia-Herzegovina), facilitating family visits (e.g., North and South Korea since 2000[409]), student exchanges and multilingual education (such as programs launched in 2011 to strengthen ties between Serbian and Albanian communities in southern Serbia[410]), and cultural or sports diplomacy (e.g., U.S.-China "ping-pong diplomacy" of the late 1960s and 1970s[411]).

[406] See here.

[407] OSCE (2012): OSCE Guide on Non-military Confidence-Building Measures (CBMs).

[408] OAS (n.d.): The Fund for Peace: peaceful settlement of territorial disputes and the role of the OAS in mediating the Belize-Guatemala territorial disput.

[409] Lee, Paul K. (2023): U.S.-North Korea Divided Families.

[410] OSCE (2012): Bujanovac's new multilingual university department: solving the language dilemma.

[411] National Museum of American Diplomacy (2021): Ping-Pong Diplomacy: Artifacts from the Historic 1971 U.S. Table Tennis Trip to China.

Acknowledgments

This analysis has been supported by the cyber diplomacy working group *Multilateral Cyber Confidence-Building Measures* and informed by additional interviews with (cyber) diplomats, researchers, and practitioners. The views and opinions expressed in this paper are those of the authors and do not reflect the official policy or position of the experts or that of their respective employer/s.

The author would like to thank all subject matter experts for their insights. In alphabetical order, acknowledging essential contributions of the members of the working group:

1. Catalina Vera Toro, Permanent Mission of Chile to the OAS
2. Eugene Tan, S. Rajaratnam School of International Studies (RSIS)
3. Folake Olagunju, Economic Community of West African States (ECOWAS)
4. Heli Tiirmaa-Klaar, IT Coalition
5. John Schabedoth, German Federal Foreign Office
6. Jörn-Arne Niemann, Permanent Mission of the Federal Republic of Germany to the OSCE
7. Julien Sylvestre-Fleury, Global Affairs Canada
8. Karsten Geier, Ständige Vertretung bei der EU & Centre for humanitarian Dialogue
9. Mariana Jaramillo, Organization of American States (OAS)
10. Moliehi Makumane, United Nations Institute for Disarmament Research (UNIDIR)
11. Neno Malisevic, Microsoft
12. Pablo Andrés Castro Hermosilla, Ministry of Foreign Affairs Chile
13. Pavlina Pavlova
14. Raphael Pfautsch, Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (GiZ)
15. Serge Droz, Swiss Federal Department of Foreign Affairs
16. Thomas Reinhold, Peace Research Institute Frankfurt (PRIF)

At *interface*, the author thanks Sven Herpig for his thoughtful guidance, Luisa Seeling for her editorial support, Alina Siebert for shaping the paper's layout, Christina Rupp for her helpful feedback on the first draft, and Iana Pervazova for helping to share this publication.

This project was funded by the German Foundation for Peace Research (DSF).

DSF
Deutsche
Stiftung
Friedensforschung
german foundation for peace research

About the Author

Helene Pleil

Helene Pleil is a Senior Policy Researcher in *interface's* Cybersecurity Policy and Resilience programme. Her research focuses on issues of cyber diplomacy, especially with regard to confidence-building measures in cyberspace, focusing on international multilateral organisations.

She holds a Master's degree in Peace and Conflict Studies from the Goethe University Frankfurt and the Technical University Darmstadt. In her master thesis she dealt with the challenges of arms control in cyberspace and in this context with the Chemical Weapons Convention. Her thesis was awarded the IANUS prize for scientific and technical peace and conflict research at the Technical University of Darmstadt and later published. She also holds a bachelor's degree in political science from Goethe University Frankfurt.

Prior to joining *interface*, Helene worked at the Digital Society Institute, ESMT Berlin, where she was responsible for numerous projects and high-level events regarding cyber policy and cyber diplomacy, for example a 1.5 diplomacy track on cybersecurity.

She also gained work experience at the Cyber Foreign Policy Coordination Staff of the German Foreign Office, at Deloitte in Public Sector Advisory on Cyber Strategy, PEASEC, an interdisciplinary research institute on technical peace research, and the Schader Foundation.

Contact

Helene Pleil
Senior Policy Researcher Cybersecurity Policy and Resilience
hpleil@interface-eu.org

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org

T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
c/o Publix
Hermannstraße 90
D-12051 Berlin

Layout
Alina Siebert

Design by Make Studio
www.make.studio

Code
Convoy Interactive